Ein Grid-basiertes, föderiertes Intrusion Detection System zur Sicherung der D-Grid Infrastruktur (GIDS)

Anforderungs- und Kriterienkatalog (MS 6)
Meilenstein zum Abschluss der Arbeitspakete 1 und 2

Öffentliche, gekürzte Version

Autoren:

Dr. Helmut Reiser	(Leibniz-Rechenzentrum Garching)
Dr. Nils gentschen Felde	(Ludwig-Maximilians-Universität München)
Felix von Eye	(Leibniz-Rechenzentrum Garching)
Jan Kohlrausch	(DFN-CERT GmbH)
Christian Szongott	(Regionales Rechenzentrum für Niedersachsen)

GEFÖRDERT VOM

Inhaltsverzeichnis

Kapitel 1

Einleitung

Dieses Dokument präsentiert als zusammenfassendes Ergebnis der ersten beiden Arbeitspakete des Projekts „Ein Grid-basiertes, föderiertes Intrusion Detection System zur Sicherung der D-Grid Infrastruktur“ (GIDS) einen Anforderungs- und Kriterienkatalog zur Auswahl und Bewertung von Intrusion Detection Systemen (IDS) für Grids. GIDS (`http://www.grid-ids.de`) ist ein Teilprojekt im Rahmen des D-Grid (`http://www.d-grid.de`) und wird vom Bundesministerium für Bildung und Forschung (BMBF, `http://www.bmbf.de`) gefördert. Weitere Projektinformationen und Unterlagen können der Projekt-Webseite entnommen werden.

1.1 Problemstellung

Im Umfeld von Grids ergeben sich im Vergleich zu konventionellen vernetzten Systemen eine Reihe bisher ungelöster Probleme, die es im Falle des D-Grid zu bewältigen gilt. So begegnet man im Grid-Kontext unter anderem einem sehr dynamischen Umfeld. Dieses ist unter verschiedenen Gesichtspunkten festzustellen, wie zum Beispiel an einer hohen Dynamik an verfügbaren Ressourcen oder auch an hoch dynamischen Nutzergruppen beziehungsweise Virtuellen Organisationen (VO). Dies erfordert individuelle, dynamische Nutzersichten, die sich in den Kontext einer VO einbetten und deren individuellen Bedürfnissen nachkommen. Weiter ergibt sich ein Grid-typisch heterogenes Umfeld. Auch dies existiert auf mehreren Ebenen und ist unter anderem auch im Bereich der Ressourcen, der eingesetzten Grid-Middleware oder auch bei den eingesetzten Grid-Diensten zu beobachten. Nicht zuletzt die zum Teil bereits von den beteiligten Organisationen eingesetzten Sicherheitskomponenten und -werkzeuge zur Erkennung von Angriffen sind von unterschiedlichster Art.

Hier ist häufig keine Koppelung bestehender Komponenten möglich und der Grid-weite Austausch von Informationen bezüglich sicherheitsrelevanter Ereignisse wird nicht umgesetzt. Dies ist nicht nur auf die Heterogenität in diesem Umfeld zurückzuführen, sondern auch auf Randbedingungen wie beispielsweise unterschiedliche Sicherheits- und Informationsverbreitungsrichtlinien („security and information sharing policies“) der beteiligten realen Organisationen. Darüber hinaus bieten Firewalls derzeit keinen umfassenden Schutz für Grids. Aufgrund fehlender Mechanismen zur dynamischen Erkennung und Freischaltung von Kommunikationsanforderungen müssen große Portbereiche zum Teil sogar ohne einschränkende Angabe von IP-Adressen permanent freigegeben werden.

Zurzeit existiert kein Gesamtkonzept für ein kooperatives, Grid-weit föderiertes Intrusion Detection System (GIDS) mit entsprechenden Reporting-Komponenten, das sich in ein Umfeld wie dem D-Grid einbettet. Daher soll ein Konzept für ein GIDS entwickelt, im D-Grid implementiert und in die Produktion überführt werden.

1.2 Ziel

Ziel dieses Projekts ist die Bereitstellung eines GIDS-Dienstes für das D-Grid. Hierbei gilt es, soweit wie möglich bestehende Ansätze zu integrieren und ein domänen- und organisa-

tionsübergreifendes Gesamtsystem zu entwickeln. Insbesondere die Fähigkeit, mit Virtuellen Organisationen (VO) umzugehen und diese auch als Kunden in Betracht zu ziehen, ist dabei von entscheidender Bedeutung. Die Grundidee ist es, Angriffe durch die kooperative Nutzung und Auswertung von lokalen Sicherheitssystemen zu erkennen. Dazu ist der Austausch von Angriffsdaten und somit deren datenschutzkonforme Aufarbeitung, auch zur Wahrung individuell bestehender Sicherheits- und Informationsverbreitungsrichtlinien, notwendig. In einem kooperativen IDS besteht die Möglichkeit, Angriffe schneller zu erkennen, als dies mit unabhängigen und nur die lokale Sicht berücksichtigenden Sicherheitssystemen möglich ist. Somit kann eine Verkürzung der Reaktionszeit der beteiligten Parteien erzielt werden. Weiter können Vorwarnungen, an zum Zeitpunkt der Erkennung eines Angriffs noch nicht betroffenen Parteien, herausgegeben sowie gegebenfalls präventive Gegenmaßnahmen ergriffen werden.

Eine Auswertung der Daten kann sich zu großen Teilen auf bereits vorhandene Ansätze klassischer IDS stützen. Bei der Auswertung der verfügbaren Datengrundlage ist darauf zu achten, dass VO-spezifische Zugriffsrechte und Befugnisse eingehalten werden. Nach erfolgreicher Auswertung aller verfügbaren Informationen durch ein kooperatives und föderiertes GIDS, unter Beachtung individueller Sicherheits- und Datenschutz-Policies, erfolgt eine Berichterstattung über die erkannten Angriffe auf das Grid oder einzelne beteiligte Partner. Auch hier ist es von Bedeutung, dass eine VO-spezifische Sicht auf die bereitgestellten Informationen realisiert wird. Dazu ist eine Anbindung an die im D-Grid bestehenden VO Managementsysteme zu schaffen. Nach der Entwicklung einer geeigneten Architektur für ein kooperatives und föderiertes IDS in Grid-Umgebungen steht die Implementierung und Produktivführung des Systems. Es soll nach Abschluss der Projektlaufzeit ein produktives Intrusion Detection System als Grid-Dienst im D-Grid zu Verfügung stehen, das sowohl von Ressourcenanbietern als auch von Kunden (VOs, Communities etc.) genutzt werden kann.

1.3 Struktur des Dokuments

Zu Beginn des Projekts wurde eine Umfrage innerhalb des D-Grids zur Bestandsaufnahme durchgeführt. Die Umfrage ist durch ein Web-basiertes Portal realisiert worden, und die Ergebnisse werden in Kapitel 2 dargestellt. Die Umfrage gliedert sich in zwei Teile: Zum einen sind Fragen zur bestehenden Netzinfrastruktur und zum anderen zu den verfügbaren Grid-Diensten gestellt worden.

Nachgelagert an die Bestandsaufnahme in Form einer Umfrage stellt Kapitel 3 eine Anwendungsfall-getriebene Anforderungsanalyse für den Fall D-Grid vor, bevor in Kapitel 4 eine Bedrohungsanalyse durchgeführt wird. Dabei orientiert sich die Vorgehensweise der Anwendungsfall-getriebenen Anforderungsanalyse an etablierten Methoden des Objektorientierten Software-Entwurfs, während sich die Bedrohungsanalyse auf Methoden des Security Engineerings stützt.

Abschließend stellt Kapitel 5 themenverwandte Arbeiten im Bereich von Intrusion Detection Systemen vor und gibt Hinweise auf ihre Eignung für den Einsatz im (D-)Grid. Dabei behandelt Kapitel 5.1 wissenschaftliche und akademische Ansätze und ihre gegebenfalls existierenden Implementierungen, während Kapitel 5.2 sich mit anderen bestehenden Produkten und Implementierungen auseinandersetzt.

Kapitel 2

Bestandsaufnahme

2.1 Einleitung und Erläuterungen

Die IT-Infrastruktur im D-Grid ist sehr vielfältig. Nicht nur die verwendeten Systeme mit unterschiedlicher Rechenpower und Anbindung sind sehr heterogen, sondern auch die verwendete Soft- und Middleware. Um einen groben Überblick zu erhalten, mit welchen Gegebenheiten das Projekt GIDS zu rechnen hat, wurden zwei anonyme Umfragen unter den Ressourcenanbietern durchgeführt, deren Ergebnisse im Folgenden erläutert werden. Die erste Umfrage *Grid-Dienste* hatte als Thema eine allgemeine Übersicht der verwendeten Middleware und Betriebssysteme, sowie der Nutzer und Dienste des Grids. Die zweite Umfrage *Sicherheitskomponenten und Netzstruktur* beleuchtet die im D-Grid vorhandenen Sicherheitskomponenten. Diese Umfrage ist insoweit interessant, da sich das zu entwickelnde Grid-basierte IDS an vorhandene Sicherheitskomponenten anpassen können muss.

Beide Umfragen wurden unabhängig voneinander durchgeführt. Daher kommen beide Umfragen bei der Frage „*Wie viele Grid-Knoten stellt Ihre Institution im D-Grid zur Verfügung?*“ zu unterschiedlichen Ergebnissen, wie in den Abschnitten 2.2.1 und 2.3.1 zu sehen.

In Kapitel 2.2 wird die erste Umfrage *Grid-Dienste* vorgestellt und in Kapitel 2.3 die Umfrage *Sicherheitskomponenten und Netzstruktur*. Dabei repräsentieren die einzelnen Unterkapitel die Fragen der Umfrage, wobei teilweise thematisch gleiche Fragen in einem Unterkapitel zusammengefasst werden.

2.2 Grid-Dienste

2.2.1 Wie viele Grid-Knoten stellt Ihre Institution im D-Grid zur Verfügung?

Die Anzahl der Grid-Knoten, die die befragten Ressourcenanbieter dem D-Grid zur Verfügung stellen, ist bei den verschiedenen Partnern sehr unterschiedlich. Während einige Anbieter nur sehr wenige Knoten dem Grid zur Verfügung stellen, sind auch andere dabei, die eine große Anzahl beisteuern. Die Antworten auf diese Frage sind im Bereich zwischen 1 und 2200 und der Durchschnitt liegt bei 355,2. Die breite Spanne der Antworten sieht man auch direkt im Vergleich zwischen dem Durchschnittswert und den Verteilungen der Antworten (vergleiche dazu Abbildung 2.1). Während etwa die Hälfte der Befragten angegeben hat, dass die Anzahl der Grid-Knoten zwischen 1 und 50 liegt und nur bei etwa 20 Prozent der Befragten mehr als 251 Knoten existieren, liegt die durchschnittliche Anzahl doch in diesem Bereich.

2.2.2 Welche Betriebssysteme verwenden Sie in Ihrer produktiven IT-Infrastruktur?

Auf den im Grid verwendeten Servern laufen viele unterschiedliche Linux-Distributionen. Die am häufigsten genannte Distribution ist Scientific Linux, wobei auch SuSE Linux Enterpri-

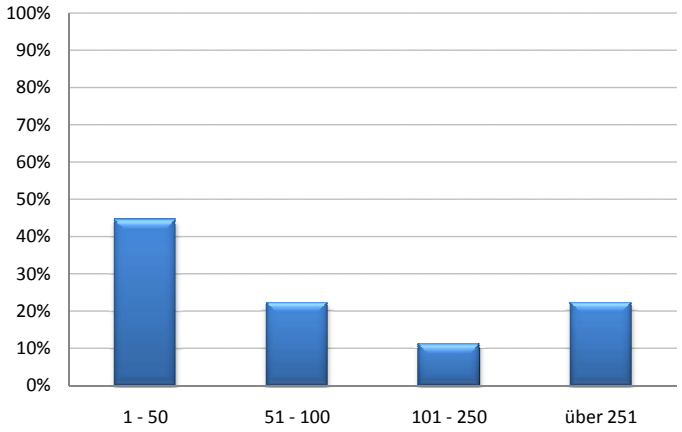

Abbildung 2.1: Prozentuale Übersicht über die Anzahl der Grid-Knoten bei der Umfrage *Grid-Dienste*

se Server häufig genannt werden. Das neben diesen beiden Distributionen auch noch einige andere laufen, wie zum Beispiel AIX, Debian Etch, Fedora Core 6 oder Ubuntu/Debian unterstreicht die hohe Heterogenität der D-Grid-Landschaft. Ein Grund, warum auch bei den einzelnen Distributionen viele verschiedene Versionen auch parallel verwendet werden, ist, dass einige Dienste in bestimmten Versionen nicht oder nur unzureichend laufen. Weiterhin ist ein Update eines Systems im laufenden Betrieb immer problembehaftet, da entweder nötige Reboot-Ausfälle durch permanente Auslastung der Systeme nicht durchgeführt werden können oder sich Konfigurationen von einzelnen Paketen ändern, so dass mögliche neue Fehlerquellen provoziert werden. Diese fehlenden Updates sind jedoch für die Gesamtsicherheit des D-Grid von entscheidender Bedeutung, da gerade bei Kernel-Updates jedes Mal zahlreiche Lücken geschlossen werden. Sind nun ein oder mehrere Systeme mit veralteten Kernel-Versionen im Grid vorhanden, so sind diese ein potentielles Einfalltor für Hacker, die dann von dieser Position aus die Vertrauensstruktur innerhalb des Grids ausnutzen können, um andere Ressourcen zu kompromittieren.

Die Aufgabe eines Grid-basierten IDS muss daher auch darin bestehen, Angriffsversuche auf diese Lücken zu erkennen und optimalerweise in Echtzeit an die zuständigen Administratoren weiterzumelden, so dass zeitnah Gegenmaßnahmen ergriffen werden können.

Scientific Linux

In der Linux-Distribution Scientific Linux sind viele verschiedene Versionen im D-Grid im Einsatz. Hauptsächlich werden offenbar die Versionen 4 und 5 beziehungsweise ihre Unterversionen eingesetzt, vereinzelnd trifft man jedoch auch noch auf Installationen der Version 3. Abbildung 2.3 zeigt die Verbreitung der einzelnen Versionen von Scientific Linux.

SuSE Linux Enterprise Server

Auch in der Linux-Distribution SuSE Linux Enterprise Server sind mehrere verschiedene Versionen im Einsatz. Dabei werden die Versionen 10 und 11 eingesetzt. Ebenso wie bei Scientific Linux wird in der unterschiedlichen Systemlandschaft auch der Grund liegen, dass bestimmte Dienste gewisse Betriebssystemanforderungen haben. Abbildung 2.3 zeigt die Verbreitung der einzelnen Versionen von SuSE Linux Enterprise Server.

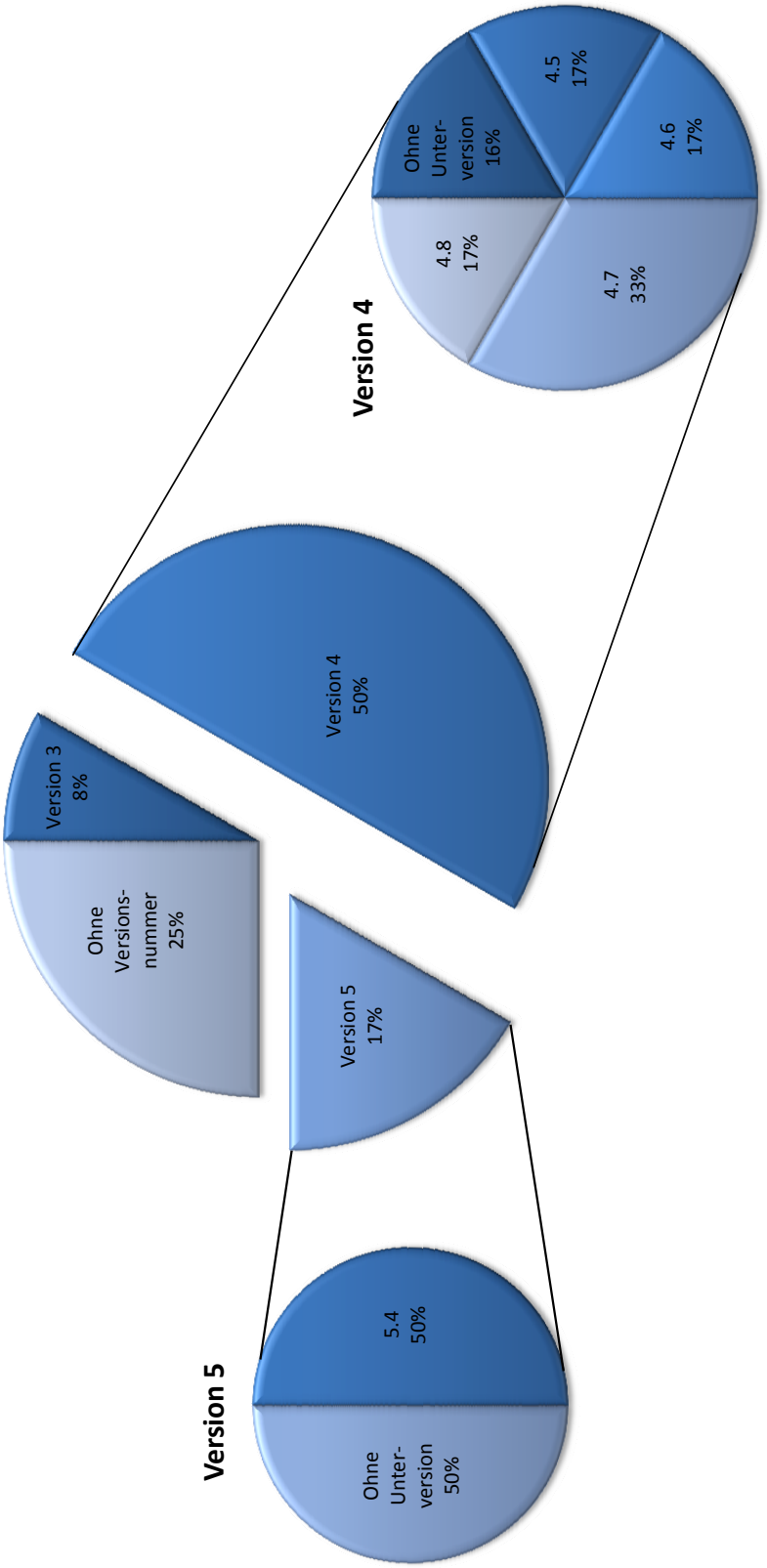

Abbildung 2.2: Versionsübersicht von Scientific Linux

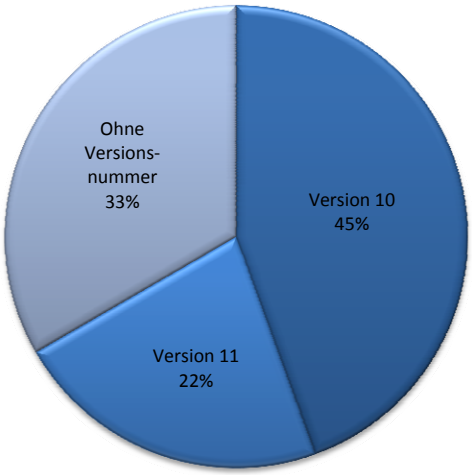

Abbildung 2.3: Versionsübersicht von SuSE Linux Enterprise Server

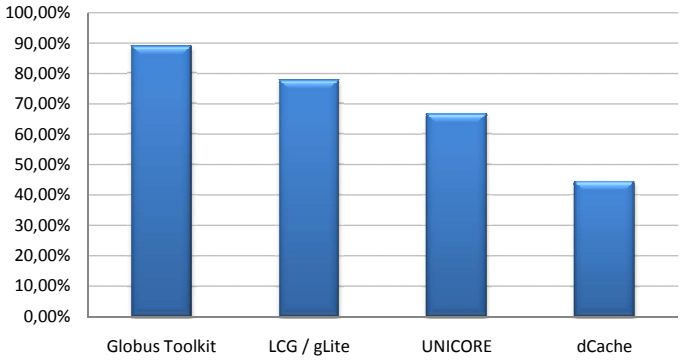

Abbildung 2.4: Einsatzverbreitung der verschiedenen Grid-Middlewares

2.2.3 Welche Grid-Middlewares betreiben Sie produktiv und in welcher Version?

Im Bereich der Grid-Middlewares gibt es im D-Grid ein breites Spektrum. Hauptsächlich sind die Middlewares Globus Toolkit, LCG / gLite, UNICORE und dCache im Einsatz. Abbildung 2.4 zeigt die Verbreitung der oben genannten Grid-Middlewares bei den befragten D-Grid-Partnern. Sehr gut erkennbar ist, dass alle Middlewaresysteme weit über 25 Prozent verbreitet sind. Dies liegt darin begründet, dass die meisten Ressourcenanbieter mehrere Middlewaredienste betreiben. Weiterhin sind auch, wie bei den Betriebssystemen, verschiedene Versionen der einzelnen Middleware-Dienste im Einsatz.

Die hohe Heterogenität der D-Grid-Infrastruktur kann man auch deutlich an Abbildung 2.5 erkennen, da keine Version einer Middleware eine signigikante Verbreitung im befragten D-Grid-Umfeld hat.

Globus Toolkit

Abbildung 2.6 zeigt die Verbreitung der unterschiedlichen Versionen von Globus Toolkit unter den befragten Partnern.

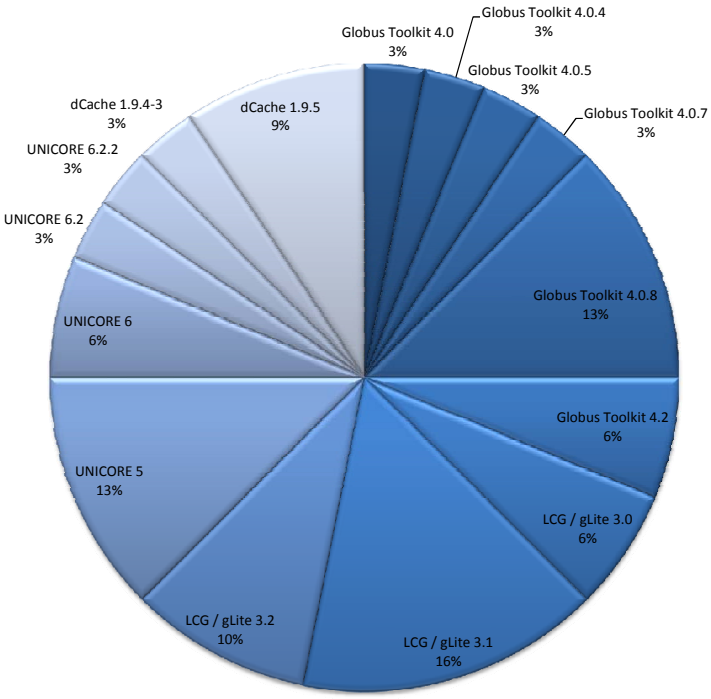

Abbildung 2.5: Einsatzverbreitung der verschiedenen Grid-Middlewares nach Versionen aufgeschlüsselt

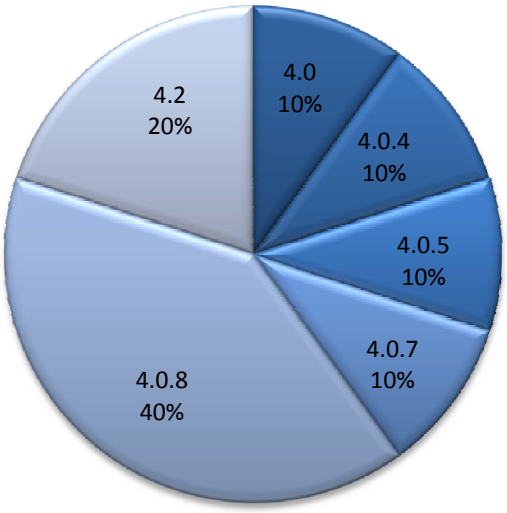

Abbildung 2.6: Versionsübersicht von Globus Toolkit

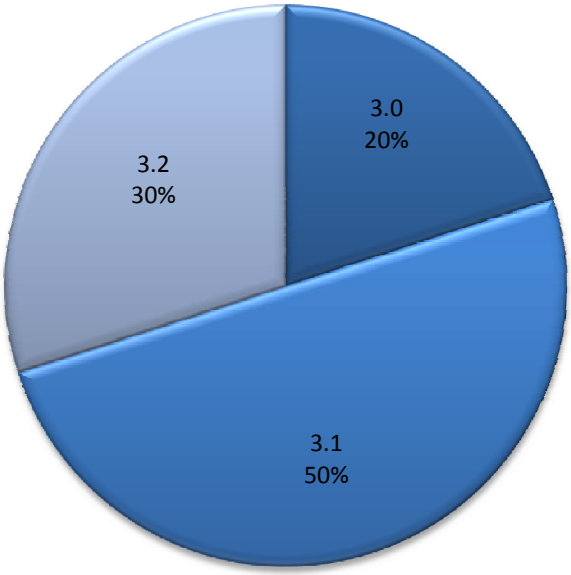

Abbildung 2.7: Versionsübersicht von LCG / gLite

LCG / gLite

Abbildung 2.7 zeigt die Verbreitung der unterschiedlichen Versionen von LCG / gLite unter den befragten Partnern.

UNICORE

Abbildung 2.8 zeigt die Verbreitung der unterschiedlichen Versionen von UNICORE unter den befragten Partnern.

dCache

Abbildung 2.9 zeigt die Verbreitung der unterschiedlichen Versionen von dCache unter den befragten Partnern.

2.2.4 Wie verwalten Sie Ihre Nutzer?

Wie an vielen Stellen auch, zeigt sich in der Nutzerverwaltung die Heterogenität der D-Grid-Landschaft. Die befragten Partner benutzen beispielsweise weitgehend standardisierte Protokolle wie Lightweight Directory Access Protocol (LDAP) oder haben eigene Systeme entwickelt. Im Gegensatz zu den offensichtlichen Heterogenitäten bei Betriebssystem- und Middleware-Versionen kann man jedoch wie in Abbildung 2.10 erkennen, dass zwei verschiedene Nutzerverwaltungen bei etwa zwei Drittel der befragten Partnern eingesetzt werden: LDAP und lokale Accounts.

2.2.5 Welche VO-Managementsysteme setzen Sie ein?

Bei den VO-Managementsystemen haben sich laut Antworten der befragten Partner die Systeme VOMS und VOMRS gleichermaßen durchgesetzt. Einige wenige Ressourcenanbieter verzichten zusätzlich komplett auf VO-Managementsysteme. Dies ist somit eine erfreuliche weitestgehende Homogenität im D-Grid. Abbildung 2.11 zeigt die prozentuale Verteilung unter den Managementsystemen.

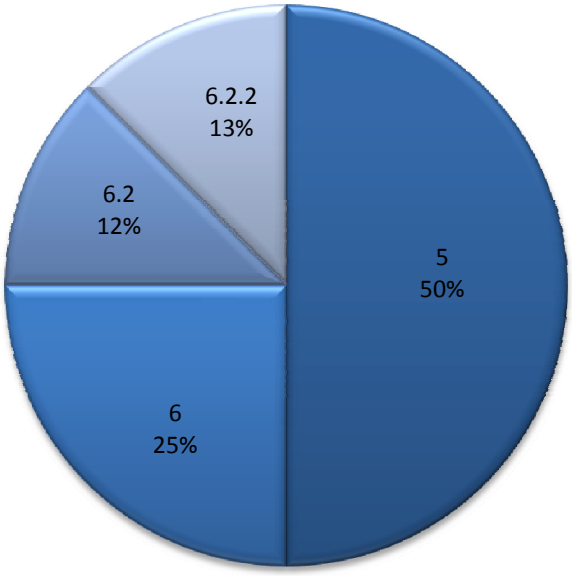

Abbildung 2.8: Versionsübersicht von UNICORE

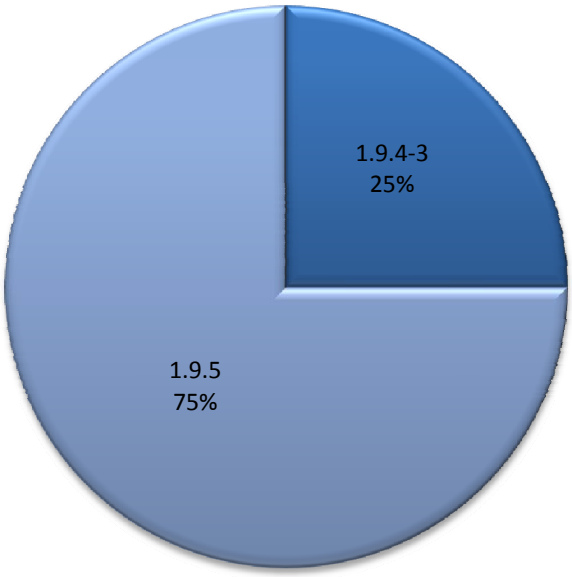

Abbildung 2.9: Versionsübersicht von dCache

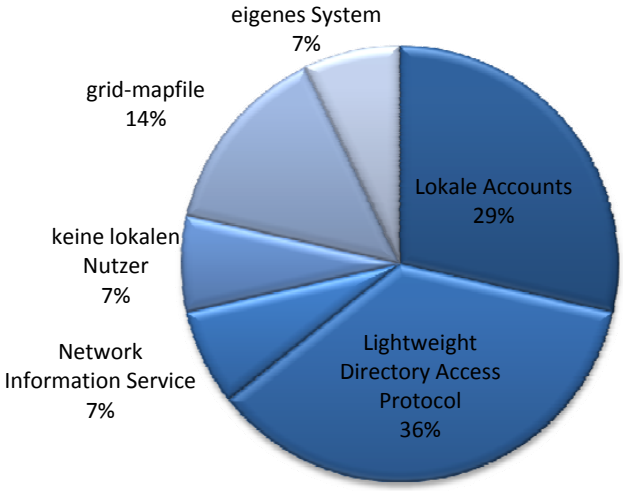

Abbildung 2.10: Verschiedene Arten der Nutzerwaltung und deren Verteilung im D-Grid

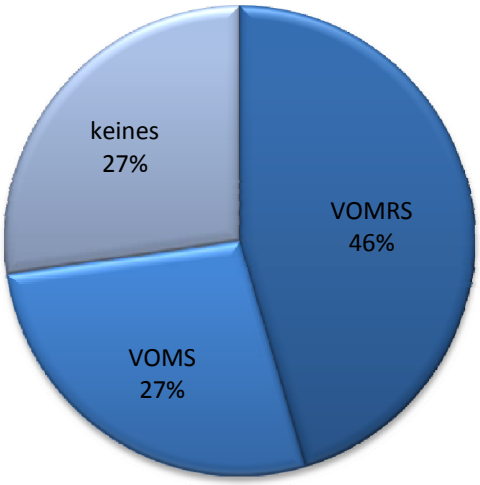

Abbildung 2.11: Übersicht über die Verteilung der im D-Grid verwendeten VO-Managementsysteme

2.2.6 Welche Grid-Dienste betreiben Sie produktiv?

Diese Frage ergibt die Erkenntnis, dass vorwiegend die Standarddienste der drei eingesetzten Grid-Middleware-Implementierungen *Globus Toolkit*, *UNICORE* und *LCG/gLite* zum Einsatz kommen. Hierbei unterscheiden sich die Antworten zum großen Teil dahingehend, dass je nach Teilnehmer der Umfrage naturgemäß ein gewisser Fokus auf die Nutzung einer speziellen Grid-Middleware liegt.

Weiter lässt sich feststellen, dass zum Teil Eigenentwicklungen, vorwiegend im Bereich Monitoring und Accounting, zum Einsatz gebracht werden. Einige Umfrageteilnehmer setzen zwar auf die im D-Grid global entwickelten und zur Verfügung gestellten Monitoring-Komponenten, es scheinen jedoch eine gewisse Anzahl an Eigenentwicklungen zu existieren. Weitere Informationen hierzu entnehmen Sie bitte auch Abschnitt 2.2.11.

Vereinzelt kommen neben den Standard-Grid-Diensten ebenfalls virtuelle Maschinen zum Einsatz. Hierbei wird vorwiegend auf den Einsatz der *Xen Grid Engine* (XGE) gesetzt.

2.2.7 Wer ist die hauptsächliche Nutzergruppe dieser Grid-Dienste?

Die hauptsächlichen Nutzergruppen der angebotenen Grid-Dienste im D-Grid sind erwartungsgemäß die im D-Grid vertretenen Virtuellen Organisationen (VO). Es gibt eine Häufung bei der Nennung des *Astro-Grid* als Hauptnutzer, was aber in diesem Fall nicht repräsentativ sein muss. Generell scheinen lediglich die wissenschaftlich orientierten Communities, die in VOs organisiert sind, auf die Grid-Dienste zuzugreifen.

2.2.8 Wie sind diese Grid-Dienste erreichbar/nutzbar?

Die Essenz der gegebenen Antworten ist, dass die im D-Grid verfügbaren Dienste im wesentlichen weltweit über das Internet erreichbar sind. Dazu werden in fast allen Fällen die Standardprotokolle der Grid-Middleware verwendet, vereinzelt werden Web-Portale zur Dienstnutzung angeboten.

2.2.9 Wird die Kommunikation spezieller Dienste verschlüsselt, da sie ansonsten unverschlüsselt erfolgen würde?

Etwa die Hälfte der Ressourcenabieter verschlüsselt die Kommunikation spezieller Dienste, vergleiche dazu Abbildung 2.12. Obwohl eine effektive Verschlüsselung von Datenströmen sehr sicherheitsrelevant ist, scheint selbst bei denjenigen, die verschlüsseln, nicht immer klar zu sein, welche Verschlüsselungsmethoden verwendet werden und an welchen Stellen die Verschlüsselung ansetzt. Jedenfalls ist nur bei wenigen Ressourcenanbietern bekannt, welche Verschlüsselung für welchen Dienst verwendet wird. Da das Projekt GIDS jedoch nur ein Baustein im Bereich Grid-Security ist, ist noch viel Überzeugungsarbeit und auch Aufklärungsarbeit nötig, eine wirklich sichere Grid-Infrastruktur zu schaffen.

2.2.10 Werden Nutzungs- und / oder Anmeldezeitpunkte protokolliert?

Standard-Logfiles werden von allen Ressourcenanbietern benutzt. Dabei verlassen sich alle mehr oder weniger auf die von den Middlewaresystemen angebotenen Logging-Mechanismen.

2.2.11 Welche Monitoring- und Accounting-Lösungen verwenden Sie?

Im Bereich des Monitoring und Accounting zeigt sich ein sehr heterogenes Bild. Zum einen setzen einige Umfrageteilnehmer auf die im D-Grid entwickelten und betriebenen Lösungen, zum anderen kommen proprietäre Produkte und Lösungen und/oder Eigentwicklungen zum Einsatz. Neben den D-Grid-weiten Monitoring-Komponenten wird vorwiegend nach auf Nagios, Ganglia sowie MDS/WebMDS gesetzt.

Abbildung 2.12: Anteil der verschlüsselten und unverschlüsselten Kommunikation im D-Grid

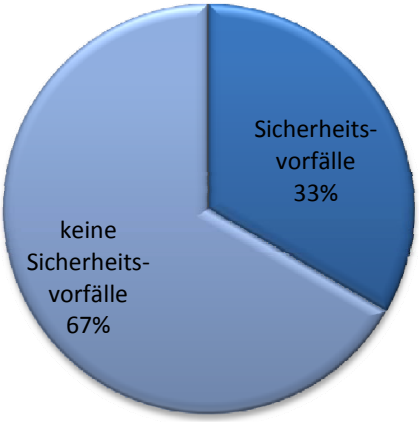

Abbildung 2.13: Anzahl der Partner mit Sicherheitsvorfällen

2.2.12 Sind in Ihrem Grid Sicherheitsvorfälle aufgetreten, die mehrere Systeme im Grid betroffen haben?

Bei etwa 30 Prozent der befragten Ressourcenanbietern, vergleiche Abbildung 2.13, wurden in der Vergangenheit Sicherheitsvorfälle aufgedeckt, die teilweise Grid-spezifische Vertrauensbeziehungen der Systeme untereinander ausgenutzen haben oder deren Angriffe Grid-spezifischen Anwendungen galt. Die Grid-Verantwortlichen haben jedoch in vielen Fällen keine Details zur Erkennung oder Behebung der Sicherheitsvorfälle von anderen Stellen erhalten. Bei den unbetroffenen Partnern ist es zwar erfreulich, dass bisher noch keine Sicherheitsvorfälle aufgefallen sind, jedoch stellt sich hier die Frage, ob mögliche Angriffe nicht stattgefunden haben oder ob, mangels eines geeigneten Systems, diese nicht als solche erkannt wurden.

2.3 Sicherheitskomponenten und Netzstruktur

2.3.1 Wie viele Grid-Knoten stellt Ihre Institution im D-Grid zur Verfügung?

Die Anzahl der Grid-Knoten, die die befragten Ressourcenanbieter dem D-Grid zur Verfügung stellen, ist bei den verschiedenen Partnern sehr unterschiedlich. Auch ist die Verteilung unterschiedlich zu den in Kapitel 2.2.1 angegebenen Werten, da vermutlich unterschiedliche Institu-

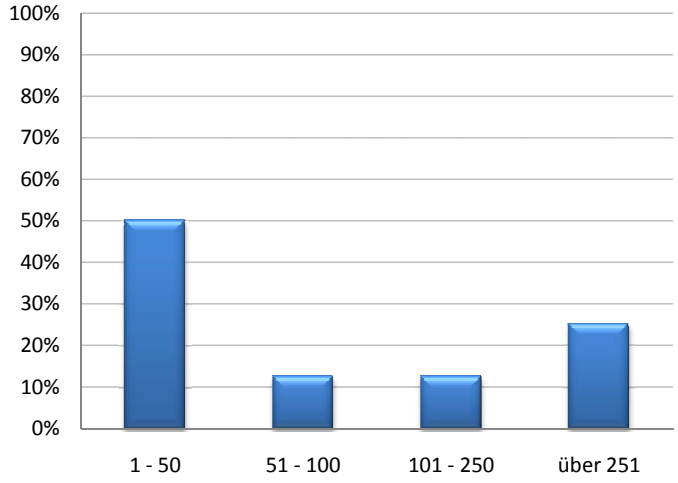

Abbildung 2.14: Prozentuale Übersicht über die Anzahl der Grid-Knoten bei der Umfrage *Sicherheitskomponenten und Netzstruktur*

tionen die beiden Umfragen ausgefüllt haben. Während einige Anbieter nur sehr wenige Knoten dem Grid zur Verfügung stellen, sind auch andere dabei, die eine große Anzahl beisteuern. Die Antworten auf diese Frage sind im Bereich zwischen 1 und 2650 und der Durchschnitt liegt bei 445,125. Die breite Spanne der Antworten sieht man auch direkt im Vergleich zwischen dem Durchschnittswert und den Verteilungen der Antworten (vergleiche dazu Abbildung 2.14). Während genau die Hälfte der Befragten angegeben hat, dass die Anzahl der Grid-Knoten zwischen 1 und 50 liegt und nur bei einem Viertel der Befragten mehr als 251 Knoten existieren, liegt die durchschnittliche Anzahl doch deutlich in diesem Bereich.

2.3.2 Welche Router betreiben Sie in Ihrem Netz?

Bei den Routern hat sich die Firma Cisco einen Marktanteil von fast zwei Drittel unter den befragten Partnern. Dies hat den Vorteil, dass die Anbindungen von GIDS an die meisten Router über standardisierte oder quasi-standardisierte Protokolle und Schnittstellen ablaufen kann. Abbildung 2.15 zeigt die Verteilung der Cisco-Router im Vergleich zu allen anderen Herstellern.

2.3.3 Zeichnen Sie Netflow-Traces auf?

Zur Analyse von Angriffen oder Angriffsversuchen ist es wichtig, umfassende Netzverbindungs- und Netzzugriffsdaten bereitzuhalten. Eine Möglichkeit, diese Daten zu protokollieren, ist Netflow-Traces aufzuzeichen. Dass, wie auf Abbildung 2.16 zu sehen, fast zwei Drittel der befragten Ressourcenanbieter diese Art der Protokollierung einsetzen, ist sehr positiv zu bewerten, da auf diesen Daten aufbauend eine umfassende Analyse des Netzverkehrs möglich ist. Beim restlichen Drittel der Befragten muss im Einzelfall geklärt werden, ob das Aufzeichnen von Netflow-Traces mit den vorhandenen Sicherheits- und Datenschutz-Policies vereinbar ist oder ob äquivalente Daten gesammelt werden können.

2.3.4 Welche Firewalls betreiben Sie in Ihrem Netz und an welchen Stellen?

Bei den Firewalls ergibt sich wieder ein sehr heterogenes Bild in der D-Grid-Landschaft. Zwar wird auch hier, wie auch bei den Routern, häufig auf die Produkte der Firma Cisco zurückgegriffen und die Firewall steht zumeist am Übergang vom X-Win zum Cluster. Jedoch sind auch

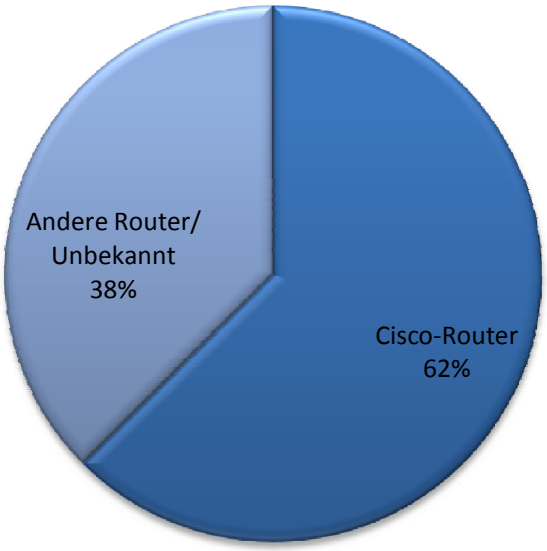

Abbildung 2.15: Cisco-Router im D-Grid

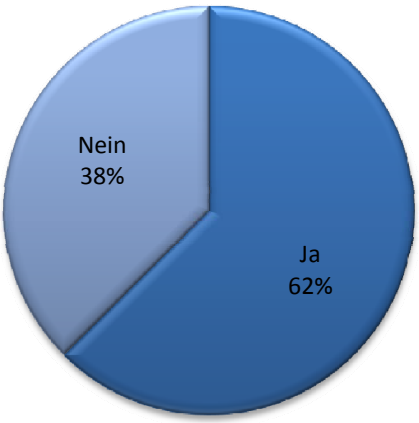

Abbildung 2.16: Antworten auf die Frage: „Zeichnen Sie Netflow-Traces auf?“

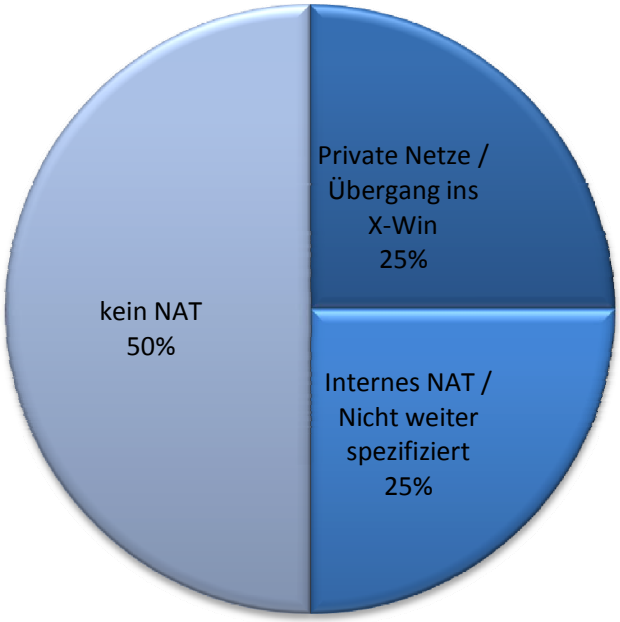

Abbildung 2.17: Verwendung von Network Adress Translation bei den befragten Partnern

diverse Personal Firewalls im Einsatz oder auch Firewalls, die an anderen Stellen stehen und nicht nur am Gateway. Für ein Grid-basiertes IDS bedeutet dies, dass es mit verschiedenen Konfigurationen und damit auch mit Daten- und Kommunikationsmodellen von unterschiedlicher Qualität und Quantität umgehen muss.

2.3.5 Setzen Sie Network Adress Translation (NAT) ein und wenn ja, in welchen Netzen?

Bei der Analyse von Logdaten ist es wichtig zu wissen, woher Netzwerkanfragen kommen und welches Zielsystem dabei angesprochen wird. Mit Hilfe von Network Adress Translation (NAT) ist es möglich, diese Daten zu verändern, um so beispielsweise ein privates Netz hinter einem Router zu betreiben. Jedoch muss bei der Analyse der Logfiles bekannt sein, ob die Daten manipuliert wurden und bestenfalls, welche Zielsysteme ursprünglich gemeint waren. Abbildung 2.17 zeigt die Verbreitung von NATs im D-Grid. Dabei sind gerade die NAT-Systeme, die am Übergang zum X-Win stehen problematisch, weil man unter Umständen bei einem Angriff kein spezielles Zielsystem mehr indentifizieren kann.

2.3.6 Setzen Sie IPv6 ein und wenn ja, in welchen Netzen?

Die Durchdringung von IPv6 ist unter den befragten Partnern noch sehr verbesserungswürdig. Nur ein einziger Ressourcenanbieter benutzt für diverse Dienste IPv6, während alle anderen noch auf IPv4 setzen.

2.3.7 Betreiben Sie Intrusion Detection Systeme (IDS) und wenn ja, welche?

Intrusion Detection Systeme (IDS) werden nur bei etwa der Hälfte der Ressourcenanbieter benutzt, vergleiche Abbildung 2.18. Bei denjenigen, die ein IDS zur Sicherung ihrer Infrastruktur benutzen, sind viele Eigenentwicklungen zu finden. Nachteilig in diesem Zusammenhang ist, dass kein Produkt bei mehr als einem Anieter zu finden ist. Somit muss man bei der Entwicklung eines Grid-basierten IDS nicht nur diejenigen ausstatten, die noch gar kein IDS

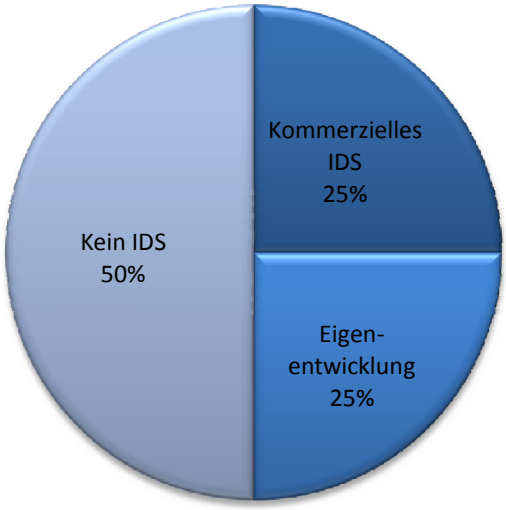

Abbildung 2.18: Verbreitung von Intrusion Detection Systemen im D-Grid

betreiben, sondern muss auch zusätzlich noch auf alle Besonderheiten der verschiedenen im D-Grid vorhandenen Systeme eingehen.

2.3.8 Setzen Sie Proxies ein und wenn ja, welche Proxies und für welche Dienste?

Im befragten D-Grid-Umfeld werden nur vereinzelnd Proxies verwendet, beispielsweise um den Zugriff auf Bibliotheken und digitale Zeitschriften über ein Application Level Gateway zu ermöglichen oder um den Internetverkehr zu steuern und zu reduzieren. Direkt im Grid wird jedoch kein Proxy verwendet.

2.3.9 Welche Viren-Scanner betreiben Sie in Ihrem Netz?

Abbildung 2.19 zeigt die momentane Verbreitung von Antivirussoftware bei den befragten Ressourcenanbietern. Hier zeigt sich leider, dass ein wichtiger Teil einer umfassenden Sicherheitsstrategie von vielen Providern nicht unterstützt wird. Sind jedoch Virenscanner vorhanden, so können deren Logfiles mit dazu beitragen, die Erkennungsrate eines Grid-basierten IDS zu erhöhen, indem das Muster von durchgeführten und erkannten Angriffen analysiert und in das IDS eingepflegt werden. Im Gegensatz zu den meisten anderen Fragen ist jedoch in diesem Fall eine hohe Heterogenität unter den Anwendern von großem Vorteil, da die unterschiedlichen Antivirensoftwares sehr verschiedene Erkennungsraten bei Malware besitzen.

2.3.10 Welche Anti-Spam Mechanismen betreiben Sie und welche Logfiles werden von diesen erzeugt?

Spam ist in heutigen Computernetzen ein großes Problem und in vielen Statistiken wird Spam ein Anteil von 97 Prozent am E-Mailverkehr zugeschrieben. Weiterhin bindet das Annehmen, Verarbeiten, Weiterleiten oder Ablehnen von Spamnachrichten große Systemressourcen. Dass trotzdem mehr als ein Fünftel (vergleiche Abbildung 2.20) der befragten Ressourcenanbieter keine Anti-Spam Mechanismen anwenden, mag darin begründet sein, dass speziell im Grid-Umfeld keine Mailserver betrieben werden. Bei der Frage nach den Logfiles antworteten die befragten Partner sehr unterschiedlich. Etwa die Hälfte der Ressourcenprovider, die auch Anti-Spam Maßnahmen anwenden, lassen die Standardprotokollierungsprogramme mitlaufen. Der Rest lässt die Protokollierung ganz sein oder ist sich nicht sicher, ob mitprotokolliert wird.

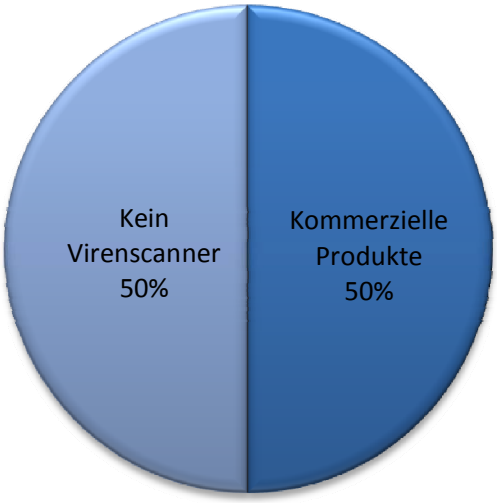

Abbildung 2.19: Antivirussoftware-Verbreitung bei den D-Grid-Partnern

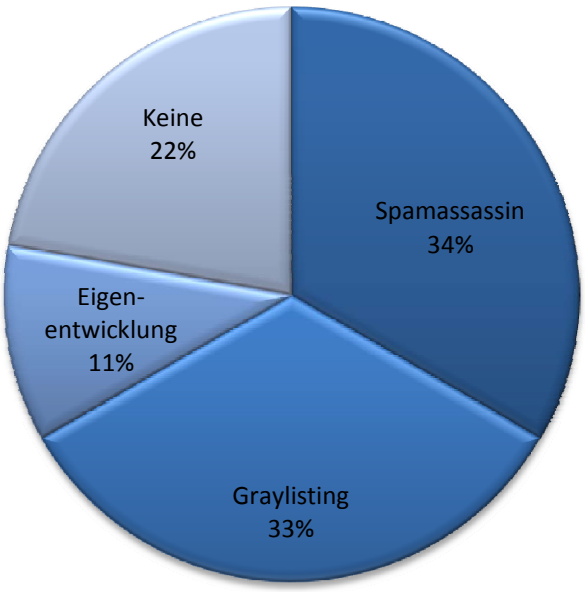

Abbildung 2.20: Anti-Spam Maßnahmen im D-Grid

2.4 Zusammenfassung

In der durchgeführten Umfrage ist erwartungsgemäß ein sehr heterogenes Bild zu Tage getreten, die sich vor allem in der großen Vielfalt an Diensten, Betriebssystemen und Middlewares äußert. Gerade im Bereich Sicherheit gibt es jedoch auch eine große Differenz zwischen den einzelnen Ressourcenanbietern. Auf der einen Seite bieten einige an ihren Grid-Knoten das komplette Arsenal mit Virenscanner, Firewall, IDS und Log-Analyse-Tools auf, um Angriffe abzuwehren oder zu erkennen. Auf der anderen Seite gibt es welche, die von den genannten Sicherheits-Tools keine im Grid-Cluster laufen haben und die sich einzig und alleine auf eine Firewall verlassen, die am Zugang vom X-Win zum Cluster installiert ist.

Erfreulich ist, dass man höchstwahrscheinlich auf einige Dinge zurückgreifen kann, wie zum Beispiel auf scheinbar zahlreich vorhandene Netflow-Daten. Vor allem, wenn man den Ressourcenanbietern ein schlüssiges Datenschutzkonzept präsentieren kann, wird eine Nutzung der Daten möglich sein.

Kapitel 3

Anwendungsfall-getriebene Anforderungsanalyse

3.1 Anwendungsfall-getriebene Analyse von Anforderungen

Die in den folgenden Unterabschnitten durchgeführte Anforderungsanalyse zur Erhebung von Anforderungen an Frühwarnsysteme in Grid-Umgebungen soll Anwendungsfall-getrieben erfolgen. Die dabei angewandte Methodik folgt der Vorgehensweise der objektorientierten Analyse von Anwendungsfällen (sogenannte *Use Cases*) wie auch unter anderem in [17] und [5] näher beschrieben. Der Ausgangspunkt der Anwendungsfallanalyse ist die knappe und informelle Beschreibung ausgewählter Szenarien, die aktuellen Grid-Projekten entspringen und somit einen Anspruch auf Praxisnähe erheben.

Bei der Anwendungsfallanalyse wird zuerst eine informelle Beschreibung eines Anwendungsfalls, der aus einem aktuellen Grid-Projekt entspringt, gegeben. Mittels Abstraktion und Generalisierung wird daraus ein sogenanntes *Use Case-Modell* generiert, welches aus *Akteuren* und *Anwendungsfällen* (den *Use Cases*) besteht und eine externe Sicht auf das System beschreibt. Dieses Use Case-Modell modelliert in diesem speziellen Fall das zu beobachtende System (hier also das Grid) mit Fokus auf beziehungsweise aus Sicht des beobachtenden Systems (hier also das Frühwarnsystem).

Ein *Akteur* ist in diesem Modell eine Entität, die von außen Informationen mit dem beschriebenen System austauscht. Akteure werden dabei durch ihre Rolle, die sie gegenüber dem System einnehmen, charakterisiert und im nachfolgenden jeweils (zusätzlich zu ihrer ausführlichen textuellen Beschreibung) durch eine Tabelle, wie zum Beispiel Tabelle 3.1, zusammengefasst.

Akteur *beispielhafter Akteur*	
Bezeichner	Akteur:ID
Kurzbeschreibung	An dieser Stelle steht eine Kurzbeschreibung des Akteurs
Assoziierte Anwendungsfälle	Hier stehen die assoziierten Anwendungsfälle, in die der beschriebene Akteur involviert ist.

Tabelle 3.1: Zusammenfassung des Akteurs *beispielhafter Akteur*

Der *Anwendungsfall* oder *Use Case* hingegen beschreibt auf der einen Seite funktionale Anforderungen an ein System, auf der anderen Seite beschreibt er die Interaktion zwischen Akteur(en) und dem System bei der Bearbeitung einer bestimmten Aufgabe. Nach [17] besteht eine Beschreibung eines Anwendungsfalls aus folgenden Elementen:

- Name des Anwendungsfalls
- Kurzbeschreibung
- Vorbedingung
  Die Vorbedingung ist die Voraussetzung für eine erfolgreiche Ausführung des zu beschreibenden Anwendungsfalls.
- Nachbedingung
  Die Nachbedingung ist der Zustand nach erfolgreicher Durchführung des Anwendungsfalls.
- Primärszenario
  Das Primärszenario oder auch Standardablauf bezeichnet die Schritte und Interaktionen, die im fehlerfreien Fall bei der Durchführung des Anwendungsfalls durchlebt werden.
- Sekundärszenarien
  Bei einem Anwendungsfall können mehrere Sekundärszenarien oder auch Alternativabläufe zum Tragen kommen. Dabei handelt es sich um Fehlerfälle während der Ausführung eines Anwendungsfalls und eventuell vorhandenen Optionen in einem solchen Fall.

In den nachfolgenden Unterkapiteln werden nach diesem Schema einzelne Anwendungsfälle aus dem D-Grid Projekt detailliert dargestellt und die funktionalen und nicht-funktionalen Anforderungen an ein Frühwarnsystem in Grid-Umgebungen davon abgeleitet. Zusätzlich zur ausführlichen Darstellung eines jeden Anwendungsfalls wird dieser in Form einer Tabelle, wie zum Beispiel Tabelle 3.2, zusammengefasst.

Anwendungsfall *beispielhafter Anwendungsfall*	
Bezeichner	UseCase:ID
Kurzbeschreibung	An dieser Stelle steht eine Kurzbeschreibung des Anwendungsfalls
Vorbedingung	Die Vorbedingung beschreibt die erforderlichen Voraussetzungen für eine erfolgreiche Ausführung des Anwendungsfalls.
Nachbedingung	Die Nachbedingung ist der Zustand nach erfolgreicher Durchführung des Anwendungsfalls.

Tabelle 3.2: Zusammenfassung des Anwendungsfalls *beispielhafter Anwendungsfall*

3.1.1 Allgemeine Beschreibung des „D-Grid“ Projekts

Der Grundstein für das D-Grid Projekt (`http://www.d-grid.de/`) wurde durch die Gründung der D-Grid Initiative (DGI) im Jahr 2003 gelegt. Eine Gruppe deutscher Wissenschaftler veröffentlichte ein richtungweisendes Strategiepapier [16], in welchem die aktuelle Situation des deutschen Forschungsumfelds analysiert und der zu erwartende Einfluss des Grid-Computings auf die Forschung untersucht wird. Aufgrund der elementaren Bedeutung wurde als Ergebnis der vorausgegangenen umfangreichen Arbeit ein langfristig ausgerichtetes, strategisches Forschungs- und Entwicklungsprogramm empfohlen – das D-Grid.

Diesem Vorschlag folgend begründete das Bundesministerium für Bildung und Forschung (BMBF, `http://www.bmbf.de/`) wenig später die deutsche D-Grid Initiative. Zur Förderung von Projekten aus den Bereichen e-Learning, Wissensmanagement und Grid-Computing in Form des anzustrebenden D-Grids sollten in einem Zeitraum von fünf Jahren bis zu 100 Millionen Euro bereitgestellt werden. Unter Zuhilfenahme der aufzubauenden Grid-Infrastruktur wird angestrebt, e-Science-Methoden in der deutschen Wissenschaft zu etablieren, wobei damit ein neuer Ansatz des netzbasierten wissenschaftlichen Arbeitens verfolgt wird. Auf der Basis

neuester Netztechnologien und in konsequenter Nutzung der Informations- und Wissenstechnologien werden Forschungsprozesse erleichtert, verbessert und intensiviert, indem integrierte Forschungsnetze mit hochleistungsfähigen, verteilten Rechnerressourcen und darauf aufbauenden Diensten innerhalb eines Grids bereitgestellt werden.

Im September 2005 sind neben dem Kern-D-Grid beziehungsweise dem D-Grid Integrationsprojekt sechs weitere, sogenannte Community-Projekte am Aufbau einer neuartigen, auf Nachhaltigkeit ausgelegten Grid-Infrastruktur beteiligt worden. Das Integrationsprojekt nimmt dabei die zentrale Aufgabe wahr, die vielfältigen Entwicklungen der untereinander sehr verschiedenen Community-Projekte in eine gemeinsame Plattform zu integrieren und der deutschen Wissenschaftsgemeinde als Dienste im Kern-D-Grid zugänglich zu machen. Zu den seit Anbeginn beteiligten Communities zählen dabei:

- AstroGrid-D – German Astronomy Community Grid (GACG)
- C3-Grid – Collaborative Climate Community Data and Processing Grid
- HEP-Grid – Grid-Infrastruktur für die Hochenergiephysik
- InGrid – Innovative Grid-Entwicklungen für ingenieurwissenschaftliche Anwendungen
- MediGRID – Grid-Computing für die Medizin und die Lebenswissenschaften
- TextGrid – Community-Grid für die Geisteswissenschaften

Mittlerweile ist eine Vielzahl an Communities in das D-Grid eingebunden, deren genaue Auflistung unter `http://www.d-grid.de/` verfügbar ist. In einer zweiten Entwicklungsphase (D-Grid 2, Jahre 2007-2010) kommen erweiterte IT-Dienste für Wissenschaft und Industrie hinzu, die auf der sogenannten Integrationsschicht des D-Grid aufbauen. Für die Zukunft sind noch weitere Schritte zum Ausbau der D-Grid-Infrastruktur geplant.

Eine technische Besonderheit des D-Grids ist, dass insgesamt drei verschiedene Grid-Middleware Lösungen parallel zum produktiven Einsatz kommen. So sind alle Rechnersysteme der DGI in der aktuellen Version des Globus Toolkit, LCG/gLite und UNICORE ansprechbar, es gibt dabei keine statische Systempartitionierung. Grundsätzlich stehen alle Systeme, die im D-Grid zum Einsatz kommen, jedem Teilnehmer am D-Grid zur Verfügung. Eine Ausnahme bilden dabei Sicherheitsprobleme oder Missbrauch im Einzelfall. An die Nutzung der Ressourcen im D-Grid sind keine Vorbedingungen geknüpft, die über die allgemeinen Vorbedingungen (Beantragung und Besitz gültiger Zertifikate) zur Teilnahme am Grid hinausgehen. Dies impliziert, dass sogar Nutzer außerhalb von D-Grid diese Ressourcen verwenden dürfen, jedoch haben sie eine geringere Priorität als jeder D-Grid Teilnehmer [8].

3.1.2 Nutzergruppen- und Kundensicht auf ein GIDS

Betrachtet man im Kontext Grid-basierter Frühwarnsysteme die potentielle Nutzergruppe beziehungsweise den Kundenkreis, so ergeben sich insbesondere Vituelle Organisationen (VO), Ressourcenanbieter sowie das Grid Operations Center (GOC) als Kandidatenmenge. Diese Menge ist abgeleitet aus den nachstehenden Anwendungsfällen, nachfolgend findet sich eine kurze Darstellung der beteiligten Akteure.

VO als Kunde. Virtuelle Organisationen beziehungsweise deren jeweilige Mitglieder oder Sub-VOs in verschiedenen Rollenausprägungen zählen zum Kundenkreis eines Grid-basierten Frühwarnsystems. Sie erwarten insbesondere eine angepasste Berichterstattung zu von der VO genutzten Ressourcen und Diensten. Des weiteren interagieren sie aber unter Umständen auch mit dem System, um möglicherweise auch Verfügbarkeiten und Service Level Agreements (SLA) mit Hilfe von historischen Daten zu überprüfen. Tabelle 3.3 fasst den Akteur „VO“ als Kunde eines Grid-basierten IDS nochmals zusammen.

Ressourcenanbieter als Kunde. Ressourcenanbieter sind direkt an einer Grid-basierten Einbruchserkennung beteiligt. Sie stellen für eine Nutzung durch das Grid Kontingente ihrer lokalen Ressourcen und Dienste zur Verfügung, die somit auch bedroht sind. Ressourcenanbieter betreiben zumeist bereits lokale IDS Instanzen, können aber maßgeblich

Akteur *VO als Kunde*	
Bezeichner	Akteur:VO:Customer
Kurzbeschreibung	Eine Virtuelle Organisation, die Informationen zur Sicherheit der von ihr genutzten Ressourcen und Dienste wünscht
Assoziierte Anwendungsfälle	*UseCase:VO:Customer* (siehe Tabelle 3.9 auf Seite 25) *UseCase:Forensik* (siehe Tabelle 3.12 auf Seite 28) *UseCase:Privacy* (siehe Tabelle 3.13 auf Seite 29)

Tabelle 3.3: Zusammenfassung des Akteurs *VO als Kunde*

auch von der Analyse übergreifender Informationen (wie sie zum Beispiel im Grid gesammelt und verarbeitet werden können) profitieren. Dabei liegt das Hauptaugenmerk auf dem aktuellen Sicherheitsstatus der eigenen Ressourcen. Zusätzlich verspricht sich ein Ressourcenanbieter von der Teilnahme an einem kooperativen Frühwarnsystem eben eine **Früh**warnung. Informationen zu gerade erfolgten Angriffen (ob erfolgreich oder nicht) können einen enormen Mehrwert für einen Betreiber bieten, als dass er daraus gegebenenfalls präventive Maßnahmen zu seinem eigenen Schutz ableiten und umsetzen kann. Tabelle 3.4 fasst einen Ressourcenanbieter als Kunde nochmals zusammen.

Akteur *Ressourcenanbieter als Kunde*	
Bezeichner	Akteur:ResProv:Customer
Kurzbeschreibung	Ein Ressourcenanbieter, der Informationen zur Sicherheit der von ihm für das Grid bereitgestellten Ressourcen und Dienste wünscht
Assoziierte Anwendungsfälle	*UseCase:Integration* (siehe Tabelle 3.8 auf Seite 24) *UseCase:ResProv:Customer* (siehe Tabelle 3.10 auf Seite 26) *UseCase:Forensik* (siehe Tabelle 3.12 auf Seite 28)

Tabelle 3.4: Zusammenfassung des Akteurs *Ressourcenanbieter als Kunde*

Grid Operations Center. In größeren Grid-Umgebungen, wie zum Beispiel dem D-Grid, wird eine zentrale Anlaufstelle, nicht zuletzt auch zur Information über die Sicherheitslage, immer häufiger gefordert und auch ins Leben gerufen [3] – ein Grid Operations Center (GOC). Prinzipiell gehört zum Tätigkeitsbereich eines GOC unter anderem auch die fortwährende Überwachung aller wichtigen Ressourcen und Dienste des Grids, speziell also auch mit Hilfe eines Grid-basierten Intrusion Detection Systems sowie auch die Überwachung des IDS selbst. Kommt es zu Ausfällen oder Fehlern (sowohl im Grid wie auch in Bezug auf ein Grid-basiertes Frühwarnsystem), koordiniert und kontrolliert das GOC die zeitnahe Wiederherstellung betroffener Komponenten beziehungsweise leistet Hilfestellung dazu. Zusätzlich kann eine zeitlich durchgehende Unterstützung von Nutzern, Virtuellen Organisationen und Ressourcenanbietern bei anstehenden Problemen und Fragen gefordert sein. Tabelle 3.5 fasst die Rolle eines GOC als Nutzer eines Grid-basierten IDS nochmals kurz zusammen.

Betreiber des GIDS. Auch für ein GIDS bedarf es eines Betreibers. Natürlich ist nicht auszuschließen, dass mehrere Instanzen eines GIDS an organisatorisch und lokal unterschiedlichen Stellen des Grids betrieben werden, jedoch wird mindestens eine Instanz benötigt, die als informierende Einheit Berichte zur Sicherheit für den gesamten Kundenkreis zur Verfügung stellt. Organisatorisch bietet sich als Betreiber zum Beispiel das Grid Operations Center an, dessen Aufgaben unter anderem eine Unterstützung von Nutzern, VOs und Ressourcenanbietern bei Problemen und Fragen sind, wozu Informa-

Akteur *Grid Operations Center*	
Bezeichner	Akteur:GOC
Kurzbeschreibung	Das Grid Operations Center (GOC), das Informationen zum Status der Sicherheit im gesamten Grid benötigt
Assoziierte Anwendungsfälle	*UseCase:Integration* (siehe Tabelle 3.8 auf Seite 24) *UseCase:GOC* (siehe Tabelle 3.11 auf Seite 27)

Tabelle 3.5: Zusammenfassung des Akteurs *Grid Operations Center*

tionen des GIDS mitunter von Nöten beziehungsweise hilfreich sein können. Tabelle 3.6 fasst die Rolle eines Betreibers des GIDS als Nutzer eines Grid-basierten IDS nochmals kurz zusammen.

Akteur *Betreiber des GIDS*	
Bezeichner	Akteur:GIDS:Provider
Kurzbeschreibung	Der Betreiber des GIDS und somit die zentrale Anlaufstelle für alle Teilnehmer des Grids, die eine Berichterstattung zur Sicherheit wünschen.
Assoziierte Anwendungsfälle	*UseCase:VO:Customer* (siehe Tabelle 3.9 auf Seite 25) *UseCase:ResProv:Customer* (siehe Tabelle 3.10 auf Seite 26) *UseCase:GOC* (siehe Tabelle 3.11 auf Seite 27) *UseCase:Forensik* (siehe Tabelle 3.12 auf Seite 28) *UseCase:3rdParties* (siehe Tabelle 3.18 auf Seite 32)

Tabelle 3.6: Zusammenfassung des Akteurs *Betreiber des GIDS*

Management-Plattform. In großen Systemen erwachsen in vielen Fällen eine Vielzahl an Management-Plattformen und Insellösungen für den Betrieb des Gesamtsystems. Dabei nutzen die Management-Plattformen vorhandene Informationen, wie zum Beispiel Sicherheitsinformationen des GIDS, um sie in geeigneter Weise den jeweiligen Verantwortlichen aufzuarbeiten. Bei der Konzeption einer weiteren Komponente stellt sich somit die Herausforderung, das neu zu entwickelnde System möglichst gut in die bereits vorhandenen Plattformen zu integrieren, falls dies möglich ist. Da im Grid-Umfeld diverse unterschiedliche Management-Lösungen bei den einzelnen Grid-Teilnehmern zu finden sind, ergeben sich durch diese bedingt eine Menge Anforderungen, denen ein GIDS bereits in der Konzeptionsphase begegnen muss. Tabelle 3.7 fasst die Rolle einer Management-Plattform als Nutzer eines Grid-basierten IDS nochmals kurz zusammen.

Anwendungsfall *Integration eines GIDS*

Ressourcenanbieter A sowie die Sicherheitsbeauftragten des Grid Operations Center möchten das GIDS in ihre (Site-lokal) bereits bestehenden Systeme zur Überwachung des Grids (zum Beispiel Monitoring-Systeme) integrieren. Beide verwenden jedoch dazu unterschiedliche Plattformen und möchten diese nicht aufgeben, um unter anderem die gewohnte Umgebung für ihr Personal beibehalten zu können und keine weiteren Anwendungen zu etablieren.

Primärszenario. Die von Ressourcenanbieter A sowie dem GOC eingesetzte Management-Plattform authentifiziert sich gegenüber dem GIDS und erhält von diesem für den jeweiligen Nutzer relevante Sicherheitsberichte. Gegebenenfalls ist neben der reinen Darstellung von Informationen auch eine gezielte Anfrage an das GIDS möglich, so dass vom

Akteur *Management-Plattform*	
Bezeichner	Akteur:MonSys
Kurzbeschreibung	Der Akteur „Management-Plattform“ ist im Grid-Kontext meist in mehrfacher und unterschiedlicher Instanziierung bei organisatorisch verschiedenen Parteien vorzufinden. Eine maximale Integration eines GIDS in möglichst viele Management-Plattformen stellt eine große Herausforderung dar.
Assoziierte Anwendungsfälle	*UseCase:Integration* (siehe Tabelle 3.8 auf Seite 24)

Tabelle 3.7: Zusammenfassung des Akteurs *Management-Plattform*

Anwendungsfall *Integration eines GIDS*	
Bezeichner	UseCase:Integration
Kurzbeschreibung	Kunden des GIDS möchten die bereitgestellten Sicherheitsberichte in ihre bestehenden Management-Plattformen integrieren und darüber gegebenenfalls individuelle Anfragen an das GIDS richten können
Vorbedingung	Der Kunde kann sich dem GIDS gegenüber authentifizieren und ist zur Informationsabfrage autorisiert
Nachbedingung	Berichte des GIDS werden innerhalb der Management-Anwendungen des Kunden dargestellt

Tabelle 3.8: Zusammenfassung des Anwendungsfalls *Integration eines GIDS*

Nutzer gewünschte Daten bereitgestellt werden können. Sämtliche Daten werden unter Gewährleistung der Datenintegrität und Vertraulichkeit ausgeliefert.

Abgeleitete Anforderungen.

- Integrierbarkeit in bestehende Management-Werkzeuge
- Interoperabilität
- Unterstützung etablierter Standards
- Einheitliche Schnittstellen
- Gesicherter Informationsaustausch (Integrität, Authentizität und Vertraulichkeit von Nachrichten)
- Nutzung standardisierter und einheitlicher Daten(austausch)formate
- Mandantenfähigkeit, nutzergruppenabhängige Berichterstattungen und Sichten
- Einbindung bestehender AA-Mechanismen

Beteiligte Akteure.

- Management-Plattform
- Grid Operations Center
- Ressourcenanbieter als Kunde

Tabelle 3.8 fasst den Anwendungsfall nochmals kurz zusammen.

Anwendungsfall *Zugriff einer VO als Nutzer eines GIDS*

Die Teilnehmer des Community-Projekts A benötigen stets Informationen zur Sicherheit der von ihnen genutzten Ressourcen und Dienste im Grid, da sie vertrauliche Daten im Grid verarbeiten. Im Falle von Unregelmäßigkeiten werden genauere Informationen, die den entsprechenden Sicherheitsbericht ausmachen, benötigt. In einem solchen Fall ist eine proaktive Benachrichtigung eines zuvor festgelegten Ansprechpartners des Community-Projekts wünschenswert.

Anwendungsfall *Zugriff einer VO als Nutzer eines GIDS*	
Bezeichner	UseCase:VO:Customer
Kurzbeschreibung	Eine VO wünscht einen Bericht zur Sicherheit der von ihr genutzten Ressourcen und Dienste im Grid
Vorbedingung	Ein authentifizierbares und autorisiertes Mitglied der VO möchte auf die Benutzerschnittstelle des GIDS zugreifen.
Nachbedingung	Ein Bericht zur Sicherheit liegt der VO vor.

Tabelle 3.9: Zusammenfassung des Anwendungsfalls *Zugriff einer VO als Nutzer eines GIDS*

Primärszenario. Ein Mitglied einer (Sub-)VO des Community-Projekts A authentifiziert sich gegenüber einer Benutzeroberfläche, die die aufbereiteten Berichte des GIDS darstellt. Auch der Zugriff auf historische Berichte sollte dabei möglich sein.

Sekundärszenario. Sollte ein Bericht zum Status der Sicherheit Auffälligkeiten beinhalten, so ist ein proaktiver Hinweis durch das Frühwarnsystem sinnvoll. Daraufhin sollte ein Mitglied einer (Sub-)VO des Community-Projekts A die Möglichkeit haben, weitere Informationen bezüglich der erkannten Unregelmäßigkeit und der sie ausmachenden Ursachen zu erhalten. Dazu ist unter Umständen ebenfalls ein Abgleich mit historischen Berichten und eine Recherche detaillierterer Daten notwendig, nicht zuletzt, um eine Verletzung potentiell bestehende SLAs mit Ressourcenanbietern auch von Nutzerseite her überprüfen zu können und somit Transparenz zu schaffen.

Abgeleitete Anforderungen.

- Verwendung einer einheitlichen und übersichtlichen Benutzerschnittstelle (zum Beispiel in Form eines Web-basierten Portals)
- Unterstützung Virtueller Organisationen und daraus folgend Einbindung in VO-Managementsysteme
- Mandantenfähigkeit, nutzergruppenabhängige Berichterstattungen und Sichten
- Einbindung bestehender AA-Mechanismen
- Nachvollziehbarkeit durchgeführter Anfragen
- Aussagekräftige Informationsaufbereitung
- Proaktive Benachrichtigung zuvor festgelegter Ansprechpartner über erkannte Unregelmäßigkeiten
- Nachhalten historischer Berichte
- Verschiedene Granularitätsstufen bei der Berichterstattung
- Gesicherter Informationsaustausch (Integrität, Authentizität und Vertraulichkeit von Nachrichten)
- Push- und Pull-Mechanismen für den Datenzugriff

Beteiligte Akteure.

- Virtuelle Organisation
- Grid-globaler Betreiber des GIDS

Tabelle 3.9 fasst den Anwendungsfall nochmals kurz zusammen.

Anwendungsfall *Ressourcenanbieter als Anwender*

Ressourcenanbieter A stellt eine Reihe Ressourcen und Dienste zur Nutzung im Grid bereit und partizipiert an einem Grid-weiten Frühwarnsystem. Die Sicherheitsbeauftragten des Ressourcenanbieters wünschen eine proaktive Alarmierung über im Grid erkannte Unregelmäßigkeiten sowohl in Bezug auf die von Ihnen angebotenen Ressourcen und Dienste wie auch die von anderen Ressourcenanbietern bereitgestellten, um so gegebenenfalls präventiv auf anstehende Bedrohungen reagieren zu können. Dazu werden möglichst detaillierte und präzise Benachrichtigungen sowie die Möglichkeit, aktiv in beim GIDS anfallenden Informationen durchsuchen zu können, benötigt.

Anwendungsfall *Ressourcenanbieter als Anwender*	
Bezeichner	UseCase:ResProv:Customer
Kurzbeschreibung	Ein Ressourcenanbieter möchte den Sicherheitsstatus der von ihm bereitgestellten Ressourcen und Dienste im Grid erfragen, gegebenenfalls proaktiv über Vorkommnisse alarmiert werden und aktiv die anfallenden IDS Daten durchsuchen können.
Vorbedingung	Ein authentifizierbarer und autorisierter Administrator eines Ressourcenanbieters möchte auf die Benutzerschnittstelle des GIDS zugreifen.
Nachbedingung	Ein Bericht zur Sicherheit liegt dem Ressourcenanbieter vor, möglicherweise notwendige Nachforschungen können aktiv vorgenommen werden.

Tabelle 3.10: Zusammenfassung des Anwendungsfalls *Ressourcenanbieter als Anwender*

Primärszenario. Ein Administrator oder Sicherheitsbeauftragter des Ressourcenanbieters A wird über durch das GIDS erkannte Unregelmäßigkeiten proaktiv benachrichtigt. Es besteht die Möglichkeit, dass sich ein Vertreter des Ressourcenanbieters A jederzeit gegenüber einer Benutzeroberfläche des GIDS authentifiziert und die aufbereiteten Berichte für das ganze Grid einsieht. Auch der Zugriff auf historische Berichte ist möglich.

Sekundärszenario. Sollten sicherheitsrelevante Vorkommnisse aufgetreten sein oder vermutet werden, so können die beim GIDS vorliegenden Sensordaten (aktuell und historisch in verschiedenen Detailgraden) aktiv untersucht werden.

Abgeleitete Anforderungen.

- Verwendung einer einheitlichen und übersichtlichen Benutzerschnittstelle (zum Beispiel in Form eines Web-basierten Portals)
- Mandantenfähigkeit, nutzergruppenabhängige Berichterstattungen und Sichten
- Einbindung bestehender AA-Mechanismen
- Aussagekräftige Informationsaufbereitung
- Nachhalten historischer Berichte
- Verschiedene Granularitätsstufen bei der Berichterstattung
- Proaktive Benachrichtigung zuvor festgelegter Ansprechpartner über erkannte Unregelmäßigkeiten
- Zugriffsmöglichkeit auf Sensordaten
- Archivierung von Sensordaten, unter Umständen in verschiedenen Detailgraden
- Gesicherter Informationsaustausch (Integrität, Authentizität und Vertraulichkeit von Nachrichten)
- Push- und Pull-Mechanismen für den Datenzugriff

Beteiligte Akteure.

- Ressourcenanbieter als Kunde
- Grid-globaler Betreiber des GIDS

Tabelle 3.10 fasst den Anwendungsfall nochmals kurz zusammen.

Anwendungsfall *Grid Operations Center*

Das Grid Operations Center dient als zentraler Ansprechpartner bei Fragen zum Grid. Zudem koordiniert das GOC die Wiederherstellung von Diensten im Grid und leistet hierzu gegebenenfalls Hilfestellung. Dazu benötigen die Mitglieder des GOC für den Bereich Sicherheit jeweils aktuelle Statusberichte, die in ihrem Detailgrad je nach Anfrage variieren und angepasst werden können müssen.

Anwendungsfall *Grid Operations Center*	
Bezeichner	UseCase:GOC
Kurzbeschreibung	Das GOC möchte sich ein Bild zur Sicherheitslage des Grids verschaffen. Als zentraler Ansprechpartner werden dazu hinreichend detaillierte Informationen benötigt, jedoch auf hoher Abstraktionsebene.
Vorbedingung	Ein authentifizierbares und autorisiertes Mitglied des GOC möchte auf die Benutzerschnittstelle des GIDS zugreifen.
Nachbedingung	Ein Bericht zur Sicherheitslage des gesamten Grids liegt vor.

Tabelle 3.11: Zusammenfassung des Anwendungsfalls *Grid Operations Center*

Primärszenario. Ein authentifizierbares und autorisiertes Mitglied des GOC greift auf die Benutzeroberfläche des GIDS zu und kann die aufbereiteten Berichte für das ganze Grid einsehen.

Sekundärszenario. Sollten Unregelmäßigkeiten berichtet werden, so können detailliertere Berichte angefordert und eingesehen werden. Außerdem können spezifische Anfragen formuliert und durch das GIDS bearbeitet werden.

Abgeleitete Anforderungen.

- Verwendung einer einheitlichen und übersichtlichen Benutzerschnittstelle (zum Beispiel in Form eines Web-basierten Portals)
- Mandantenfähigkeit, nutzergruppenabhängige Berichterstattungen und Sichten
- Einbindung bestehender AA-Mechanismen
- Aussagekräftige Informationsaufbereitung
- Verschiedene Granularitätsstufen bei der Berichterstattung
- Gesicherter Informationsaustausch (Integrität, Authentizität und Vertraulichkeit von Nachrichten)

Beteiligte Akteure.

- Grid-globaler Betreiber des GIDS
- Grid Operations Center

Tabelle 3.11 fasst den Anwendungsfall nochmals kurz zusammen.

Anwendungsfall *Beweissicherung & Forensik*

Ressourcenanbieter A und Projektgruppe B, die im Grid als VO modelliert ist, streiten um die Verletzung eines abgeschlossenen SLAs in Bezug auf einzuhaltende Sicherheitsmerkmale. B behauptet, dass A den geschlossenen SLA gebrochen hat und verlangt die im SLA verbrieften monetären Pönalen[1].

Anwendungsfall *Beweissicherung & Forensik*	
Bezeichner	UseCase:Forensik
Kurzbeschreibung	Ein Ressourcenanbieter und eine Projektgruppe streiten um die Verletzung eines abgeschlossenen SLAs in Bezug auf einzuhaltende Sicherheitsniveaus.
Vorbedingung	Ein SLA mit sicherheitsrelevanten und überprüfbaren Merkmalen wurde abgeschlossen.
Nachbedingung	Die Überprüfung des SLAs konnte durch die vom GIDS gelieferten Informationen erfolgen.

Tabelle 3.12: Zusammenfassung des Anwendungsfalls *Beweissicherung & Forensik*

Primärszenario. Die vom GIDS erzeugten Sicherheitsberichte, die die vermeintliche Verletzung des SLAs bezeugen, können sowohl von Ressourcenanbieter A wie auch VO B eingesehen werden. Die Berichte können unter Umständen auch vor längerer Zeit in der Vergangenheit erzeugt worden sein.

Sekundärszenario. Zur genaueren Klärung des Vorfalls können die Sensordaten, aus denen die generierten Berichte entstanden sind, eingesehen werden. Je nach Alter der Daten variiert dabei der Detailgrad der vorhandenen Informationen.

Abgeleitete Anforderungen.

- Nachvollziehbarkeit durchgeführter Anfragen
- Aussagekräftige Informationsaufbereitung
- Nachhalten historischer Berichte
- Zugriffsmöglichkeit auf Sensordaten
- Archivierung von Sensordaten, unter Umständen in verschiedenen Detailgraden
- Gewährleistung der Integrität des Datenbestands (Berichte und Sensordaten)
- Push- und Pull-Mechanismen für den Datenzugriff

Beteiligte Akteure.

- Ressourcenanbieter als Kunde
- Grid-globaler Betreiber des GIDS
- Virtuelle Organisation

Tabelle 3.12 fasst den Anwendungsfall nochmals kurz zusammen.

Anwendungsfall *Datenschutz & Vertraulichkeit*

VO A (zum Beispiel medizinische Forscher aus dem MediGrid) möchten sensible Patientendaten im Rahmen einer Studie im Grid auswerten und analysieren. Juristische Randbedingungen fordern Garantien zur Vertraulichkeit der Daten und der Einhaltung des Datenschutzes.

[1] SLAs im eigentlichen Sinne werden zurzeit im D-Grid nicht geschlossen. Es ist jedoch auch eine entgeltliche Nutzung der Grid-Infrastruktur angedacht, so dass dieser Anwendungsfall dann zum Tragen kommen könnte.

Anwendungsfall *Datenschutz & Vertraulichkeit*	
Bezeichner	UseCase:Privacy
Kurzbeschreibung	Eine VO möchte sensible Daten im Grid verarbeiten.
Vorbedingung	Juristische Randbedingungen mit Relevanz für das GIDS können formuliert und technisch durchgesetzt werden.
Nachbedingung	Eine Datenverarbeitung im Grid kann für diesen Fall ermöglicht werden.

Tabelle 3.13: Zusammenfassung des Anwendungsfalls *Datenschutz & Vertraulichkeit*

Primärszenario. Ein Beauftragter der VO A formuliert (optimalerweise in einer maschinenlesbaren Form) die für das GIDS relevanten Randbedingungen, die für eine Verarbeitung der sensiblen Patientendaten garantiert werden müssen. Diese werden durch entsprechende Mechanismen des GIDS durchgesetzt, so dass eine Datenverarbeitung im Grid ermöglicht werden kann.

Sekundärszenario. Sollte entweder eine technische Gewährleistung oder die Formulierung der Randbedingungen nicht möglich sein, so kann eine Verarbeitung der Daten im Grid nicht vorgenommen werden.

Abgeleitete Anforderungen.

- Möglichkeiten der Zugriffsbeschränkung auf jegliche Informationen im GIDS
- Anonymisierungs- oder Pseudonymisierungsmöglichkeiten inkl. einer notwendigen (maschinenlesbaren) Beschreibungsmöglichkeit
- Mandantenfähigkeit, nutzergruppenabhängige Berichterstattungen und Sichten
- Einbindung bestehender AA-Mechanismen
- Gesicherter Informationsaustausch (Integrität, Authentizität und Vertraulichkeit von Nachrichten)

Beteiligte Akteure.

- Virtuelle Organisation

Tabelle 3.13 fasst den Anwendungsfall nochmals kurz zusammen.

3.1.3 Informationsanbieter-spezifische Sicht auf ein GIDS

Auch als Informationsanbieter sind im Rahmen eines Grid-basierten IDS eine Menge Akteure denkbar. Insbesondere ergeben sich aus den nachgestellten Anwendungsfällen bereits vorhandene Host- und Netzsensorik, der Ressourcenanbieter (diesmal in der Rolle des Informationslieferanten), VOs (hier ebenfalls in der Rolle des Informationslieferanten) sowie verschiedene Drittanbieter, die ansonsten nicht weiter in die Aktivitäten des Grids eingebunden sein müssen. Nachfolgend findet sich ein kurzer Überblick über die einzelnen Akteure.

Ressourcenanbieter als Informationsanbieter. Der Erfolg sowie der sicherheitstechnische Nutzen eines Grid-basierten Frühwarnsystems, unter der Annahme, bereits vorhandene Informationen zur Sicherheit zu föderieren, hängt in hohem Maße davon ab, ob und in welcher Qualität relevante Informationen von den einzelnen eingebundenen Partnern einbezogen werden können. Insbesondere dienen in diesem Umfeld natürlich die Ressourcenanbieter auch als Informationsanbieter für ein Grid-basiertes IDS. Jedoch erheben sie gleichfalls eine Reihe Randbedingungen, die für ihre Teilnahme erfüllt sein müssen. Tabelle 3.14 fasst nochmals kurz den Ressourcenanbieter in diesem Kontext in Abgrenzung zu Unterabschnitt 3.1.2 als Informationsanbieter zusammen.

In realen Grid-Umgebungen sind Ressourcenanbieter als Informationsanbieter für ein Grid-basiertes Frühwarnsystem am häufigsten zu finden, was insbesondere durch Randbedingungen wie Datenschutzbestimmungen und die Gewährleistung der Autonomie an einem GIDS beteiligter Parteien bedingt ist. In den meisten Fällen sind Informationen von Site-spezifischen Host- und Netzsensoren zu feingranular, was meist zu Problemen in Bezug auf die Skalierbarkeit führt. Informationen, die VOs hingegen beitragen können, gehen ohnehin aus dem Aggregat der Daten aller an einem GIDS partizipierenden Parteien hervor, so dass in vielen Fällen hierdurch kein essentieller Mehrwert dargestellt werden kann.

Akteur *Ressourcenanbieter als Informationsanbieter*	
Bezeichner	Akteur:ResProv:InfoProv
Kurzbeschreibung	Ein Ressourcenanbieter, der seine Informationen über den Status der Sicherheit seiner Ressourcen (zum Beispiel IDS Daten, Firewall Logdateien etc.) einem GIDS zur Verfügung stellt
Assoziierte Anwendungsfälle	*UseCase:Autonomie* (siehe Tabelle 3.16 auf Seite 31) *UseCase:ISP* (siehe Tabelle 3.17 auf Seite 32)

Tabelle 3.14: Zusammenfassung des Akteurs *Ressourcenanbieter als Informationsanbieter*

Betreiber des GIDS. *siehe Abschnitt 3.1.2 ab Seite 21*

3^{rd} **Parties.** Auch Informationen Dritter können einen entscheidenden Einfluss auf ein Grid-basiertes IDS haben. Denkbar sind diese vor allem als externe Dienstleister. Zum Beispiel können Berichte von Computer Emergency Response Teams (CERT) zu bestehenden Sicherheitslücken und diese ausnutzende Schadprogramme sehr hilfreich bei der Einschätzung wie schwerwiegend eine Sicherheitsverletzung ist oder der Erkennung neuartiger Angriffe sein. Ein weiteres Beispiel ist der Einfluss eines Dienstleisters, der Sicherheitsprodukte, die im Grid zum Einsatz kommen, mit Aktualisierungen versorgt. Diese können sich sowohl auf die Aktualisierung der Software-Komponenten an sich (engl. *Patches*) oder auch der Aktualisierung von zum Beispiel Signaturdatenbanken eines Virenscanners oder auch IDS beziehen. Tabelle 3.15 fasst den Akteur „3^{rd} Parties“ nochmals tabellarisch zusammen.

Akteur 3^{rd} *Parties*	
Bezeichner	Akteur:3rdParties
Kurzbeschreibung	Nicht am Grid beteiligte Akteure (3^{rd} *Parties*), die relevante Informationen zur Sicherheit des Grids liefern; zum Beispiel CERTs, die Implementierungsschwächen und diese ausnutzende Schadprogramme melden
Assoziierte Anwendungsfälle	*UseCase:3rdParties* (siehe Tabelle 3.18 auf Seite 32)

Tabelle 3.15: Zusammenfassung des Akteurs 3^{rd} *Parties*

Anwendungsfall *Autonomie beteiligter Organisationen*

Ressourcenanbieter A möchte gerne verschiedene Ressourcen und Dienste im Grid zur Verfügung stellen. Dazu wird jedoch gefordert, dass A auch als Informationsanbieter für Daten zur Analyse im Rahmen des im Grid etablierten IDS auftritt. A setzt bereits verschiedene Sicherheitsmechanismen, unter anderem auch lokale IDS Instanzen, ein. Weitere (redundante)

Installationen sind nicht durchsetzbar, vielmehr sollen bestehende Komponenten und Dienste verwendet werden.

Anwendungsfall *Autonomie beteiligter Organisationen*	
Bezeichner	UseCase:Autonomie
Kurzbeschreibung	Ein Ressourcenanbieter möchte gerne an der Datensammlung für ein GIDS teilnehmen, dafür sollen jedoch bestehende Systeme genutzt und keine neuen installiert werden.
Vorbedingung	Informationen von Sicherheitsmechanismen eines Ressourcenanbieters sollen in das GIDS integriert werden.
Nachbedingung	Der Ressourcenanbieter nimmt als Informationsanbieter am GIDS teil.

Tabelle 3.16: Zusammenfassung des Anwendungsfalls *Autonomie beteiligter Organisationen*

Primärszenario. Es werden Komponenten vom Grid angeboten, die die bei Ressourcenanbieter A existierenden Informationsquellen auslesen, die Daten für das GIDS semantisch und syntaktisch aufarbeiten und in die Analyse des GIDS einbringen. Diese werden Sitelokal bei A installiert und an das Grid-weite Frühwarnsystem angebunden.

Sekundärszenario. Sollten keine geeigneten Adapter für die Systeme von A vorliegen, so besteht die Möglichkeit solche zu implementieren, da das GIDS entsprechende Erweiterungsmechanismen vorsieht.

Abgeleitete Anforderungen.

- Nutzung standardisierter und einheitlicher Daten(austausch)formate
- Unterstützung heterogener Informationsquellen
- Einheitliche Schnittstellen
- Portabilität
- Wiederverwendbarkeit bestehender Komponenten
- Interoperabilität
- Erweiterbarkeit des GIDS um bisher ungenutzte Informationsquellen zu erschließen
- Einbringen zusätzlicher Informationsquellen in das GIDS während des Betriebs

Beteiligte Akteure.

- Ressourcenanbieter als Informationsanbieter
- Betreiber des GIDS

Tabelle 3.16 fasst den Anwendungsfall nochmals kurz zusammen.

Anwendungsfall *Information Sharing Policies*

Ein Rechenzentrum tritt in der Rolle des Ressourcenanbieters A als Informationsanbieter für ein Grid-weites Frühwarnsystem auf. Rechtliche Randbedingungen zwingen A, zum Beispiel alle personenbezogenen Informationen nicht an Dritte und somit insbesondere nicht an das GIDS weiterzugeben. Außerdem äußert der Sicherheitsbeauftragte erhebliche Bedenken, sämtliche Informationen ungefiltert den am GIDS beteiligten Parteien zur Verfügung zu stellen.

Primärszenario. Ressourcenanbieter A kann ein unter seiner eigenen Administration stehendes System dazu nutzen, alle Daten, die er zur Auswertung an das GIDS weiterreichen könnte, zu filtern. Dabei ist sowohl das Aussortieren beziehungsweise Löschen als auch das Anonymisieren beziehungsweise Pseudonymisieren von Informationen möglich. Eine entsprechende Sprache zur Formulierung der Filterbedingungen wird dazu angeboten.

Anwendungsfall *Information Sharing Policies*	
Bezeichner	UseCase:ISP
Kurzbeschreibung	Durch gewisse organisatorische und rechtliche Randbedingungen kann ein Ressourcenanbieter nicht alle ihm vorliegenden Informationen zur Auswertung an ein GIDS ungefiltert weitergeben.
Vorbedingung	Ein Ressourcenanbieter möchte zum GIDS beitragen, unterliegt jedoch Auflagen bezüglich der Informationsweitergabe.
Nachbedingung	Der Ressourcenanbieter kann am GIDS partizipieren, da seine Randbedingungen technisch durchgesetzt werden können.

Tabelle 3.17: Zusammenfassung des Anwendungsfalls *Information Sharing Policies*

Sekundärszenario. Sollte Ressourcenanbieter A seine Vorgaben nicht durchsetzen können, da zum Beispiel die technischen Möglichkeiten nicht existieren, so wird er nicht am GIDS teilnehmen können.

Abgeleitete Anforderungen.

- Anonymisierungs- oder Pseudonymisierungsmöglichkeiten inkl. einer notwendigen (maschinenlesbaren) Beschreibungsmöglichkeit
- Gewährleistung der Autonomie beteiligter Informationsanbieter
- (Technische) Durchsetzung des Datenschutzes

Beteiligte Akteure.

- Ressourcenanbieter als Informationsanbieter

Tabelle 3.17 fasst den Anwendungsfall nochmals kurz zusammen.

Anwendungsfall 3^{rd} *Parties als Informationsanbieter*

Zusätzlich zu den Informationen der IDS-Sensorik im Grid sollen Daten Dritter mit in die Analyse des GIDS einfließen. Insbesondere sollen Informationen eines *Computer Emergency Response Teams* (CERT) zu bestehenden Sicherheitslücken in verwendeten Softwarekomponenten im Kontext des GIDS publik gemacht werden und Signaturen zur Erkennung von Angriffsmustern, die diese Lücken missbräuchlich ausnutzen, von einem externen Dienstleister in Form von Updates einer etablierten Signaturdatenbank übernommen werden.

Anwendungsfall 3^{rd} *Parties als Informationsanbieter*	
Bezeichner	UseCase:3rdParties
Kurzbeschreibung	Als zusätzliche Informationsquellen sollen Daten von Dritten (zum Beispiel CERTs) in die Analyse des GIDS einfließen.
Vorbedingung	In einer Anlaufstelle können Informationen und Signaturen von Dritten dem GIDS zur Verfügung gestellt werden.
Nachbedingung	Alle Teilnehmer haben ihre lokalen Daten mit den neuesten Informationen abgeglichen.

Tabelle 3.18: Zusammenfassung des Anwendungsfalls 3^{rd} *Parties als Informationsanbieter*

Primärszenario. Es steht eine Anlaufstelle im Grid bereit, die Informationen zu Sicherheitslücken im Grid und Signaturen zur Erkennung derer Ausnutzung für die eingesetzten Sicherheitssysteme bereithält. Die Teilnehmer des GIDS gleichen ihre Signaturdatenbanken regelmäßig mit den angebotenen Signaturen ab.

Abgeleitete Anforderungen.

- Nutzung standardisierter und einheitlicher Daten(austausch)formate
- Unterstützung heterogener Informationsquellen
- Einheitliche Schnittstellen
- Wiederverwendbarkeit bestehender Komponenten
- Interoperabilität
- Erweiterbarkeit des GIDS um bisher ungenutzte Informationsquellen
- Prozessspezifikation für (Signatur-)Updates der Site-spezifischen GIDS-Komponenten
- Gesicherter Informationsaustausch (Integrität, Authentizität und Vertraulichkeit von Nachrichten)
- Etablierung einer vertrauenswürdigen Koordinationseinheit im GIDS

Beteiligte Akteure.

- Grid-globaler Betreiber des GIDS
- 3^{rd} Parties

Tabelle 3.18 fasst den Anwendungsfall nochmals kurz zusammen.

3.1.4 Zusammenfassung der Akteure und Anforderungen

Die Anwendungsfall-getriebenen Anforderungsanalyse, die in diesem Abschnitt auf den Nutzerkreis und die Informationsanbieter eines GIDS fokussiert, hat insbesondere die nachfolgend aufgelisteten beteiligte Akteure hervorgebracht:

- VO als Kunde, siehe Tabelle 3.3 auf Seite 22
- Ressourcenanbieter als Kunde, siehe Tabelle 3.4 auf Seite 22
- Grid Operations Center, siehe Tabelle 3.5 auf Seite 23
- Betreiber des GIDS, siehe Tabelle 3.6 auf Seite 23
- Management-Plattform, siehe Tabelle 3.7 auf Seite 24
- Ressourcenanbieter als Informationsanbieter, siehe Tabelle 3.14 auf Seite 30
- 3^{rd} Parties, siehe Tabelle 3.15 auf Seite 30

Die Abbildungen 3.1 und 3.2 bringen nochmal zusammenfassend die jeweiligen Akteure mit den sie betreffenden Anwendungsfällen in Verbindung und stellen diese in einem UML Use Case-Diagramm dar. Abbildung 3.1 bezieht sich dabei auf die kundenspezifischen Anwendungsfälle wie sie in Abschnitt 3.1.2 zu finden sind, Abbildung 3.2 fasst die Informationsanbieter-spezifischen Anwendungsfälle aus Abschnitt 3.1.3 nochmals zusammen.

Aus der Anwendungsfall-getriebenen Anforderungsanalyse ergeben sich eine Vielzahl Anforderungen, die durch den Anwender eines GIDS sowie die Informationsanbieter bedingt sind. Die vorangehend abgeleiteten Anforderungen sind nachfolgend nochmals in einer Liste zusammengefasst aufgeführt. Die Reihenfolge der Anforderungen ist dabei alphabetisch und soll in keiner Weise eine Gewichtung oder Wertung antizipieren!

1. Anonymisierungs- oder Pseudonymisierungsmöglichkeiten inkl. einer notwendigen (maschinenlesbaren) Beschreibungsmöglichkeit
2. Archivierung von Sensordaten, unter Umständen in verschiedenen Detailgraden
3. Aussagekräftige Informationsaufbereitung

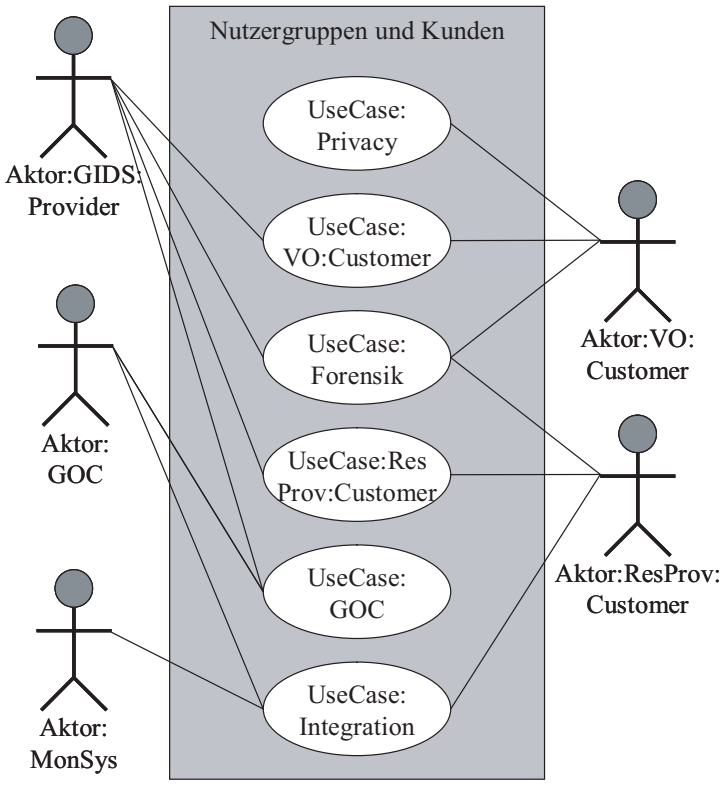

Abbildung 3.1: Übersicht der kundenspezifischen Anwendungsfälle

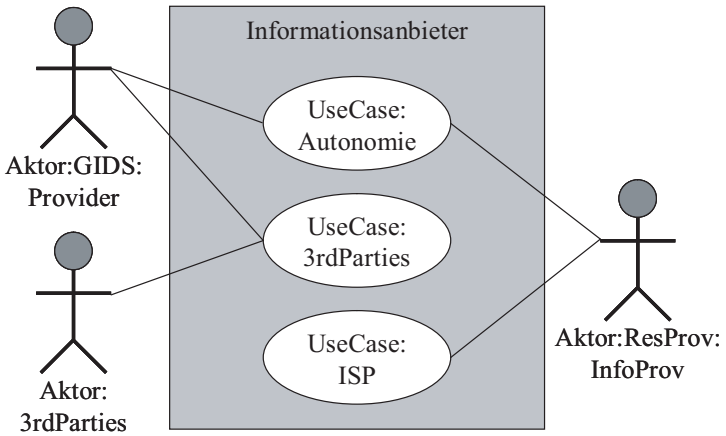

Abbildung 3.2: Übersicht der Informationsanbieter-spezifischen Anwendungsfälle

4. Einbindung bestehender AA-Mechanismen
5. Einbringen zusätzlicher Informationsquellen in das GIDS während des Betriebs
6. Einheitliche Schnittstellen
7. Erweiterbarkeit des GIDS um bisher ungenutzte Informationsquellen zu erschließen
8. Etablierung einer vertrauenswürdigen Koordinationseinheit im GIDS
9. Gesicherter Informationsaustausch (Integrität, Authentizität und Vertraulichkeit von Nachrichten)
10. Gewährleistung der Autonomie beteiligter Informationsanbieter
11. Gewährleistung der Integrität des Datenbestands (Berichte und Sensordaten)
12. Integrierbarkeit in bestehende Management-Werkzeuge
13. Interoperabilität
14. Mandantenfähigkeit, nutzergruppenabhängige Berichterstattungen und Sichten
15. Möglichkeiten der Zugriffsbeschränkung auf jegliche Informationen im GIDS
16. Nachhalten historischer Berichte
17. Nachvollziehbarkeit durchgeführter Anfragen
18. Nutzung standardisierter und einheitlicher Daten(austausch)formate
19. Portabilität
20. Proaktive Benachrichtigung zuvor festgelegter Ansprechpartner über erkannte Unregelmäßigkeiten
21. Prozessspezifikation für (Signatur-)Updates der Site-spezifischen GIDS-Komponenten
22. Push- und Pull-Mechanismen für den Datenzugriff
23. (Technische) Durchsetzung des Datenschutzes
24. Unterstützung etablierter Standards
25. Unterstützung heterogener Informationsquellen
26. Unterstützung Virtueller Organisationen und daraus folgend Einbindung in VO-Managementsysteme
27. Verschiedene Granularitätsstufen bei der Berichterstattung
28. Verwendung einer einheitlichen und übersichtlichen Benutzerschnittstelle (zum Beispiel in Form eines Web-basierten Portals)
29. Wiederverwendbarkeit bestehender Komponenten
30. Zugriffsmöglichkeit auf Sensordaten

Tabelle 3.19 stellt nochmal in einer Übersicht die je Anwendungsfall abgeleiteten Anforderungen dar. Die jeweilige Anforderungsnummer entspricht dabei der Nummerierung vorstehender Auflistung der Anforderungen, die „Nummer“ des jeweiligen Anwendungsfalls referenziert hingegen den Unterabschnitt, in dem der Anwendungsfall detailliert beschrieben ist.

Anf.-	Anwendungsfall *(siehe Abschnitt ...)*								
Nr.	3.1.2	3.1.2	3.1.2	3.1.2	3.1.2	3.1.2	3.1.3	3.1.3	3.1.3
1						✔		✔	✔
2			✔		✔				
3		✔	✔	✔	✔				
4	✔	✔	✔	✔		✔			
5							✔		
6	✔						✔		✔
7							✔		✔
8									✔
9	✔	✔	✔	✔		✔			✔
10								✔	
11					✔				
12	✔								
13	✔						✔		✔
14	✔	✔	✔	✔		✔			
15						✔			
16		✔	✔		✔				
17		✔			✔				
18	✔						✔		✔
19							✔		
20		✔	✔						
21									✔
22		✔	✔		✔				
23								✔	
24	✔								
25							✔		✔
26		✔							
27		✔	✔	✔					
28		✔	✔	✔					
29							✔		✔
30			✔		✔				

Tabelle 3.19: Übersicht der abgeleiteten Anforderungen je Anwendungsfall

3.2 Generische Anforderungen an ein GIDS

Für das Konzept eines jeden (Grid-)Systems sind eine Menge generischer Anforderungen zu beachten, die im Nachfolgenden kurz erörtert werden. Zudem ist zur Verfolgung des Ziels, ein kooperatives Frühwarnsystem für Grid-Strukturen zu entwerfen, eine Kooperation unterschiedlicher Organisationen miteinander von Nöten, die Vertrauensbeziehungen unterhalb der beteiligten Organisationen impliziert. Diesen beiden Tatbeständen wird in den Abschnitten 3.2.2 und 3.2.3 Rechnung getragen.

3.2.1 Generische Anforderungen

Bereits bei der allgemeinen Beschreibung der Konzepte und Architektur im Grid nach [12] kommen einige Anforderungen an Systeme im Grid bzw. ihre Eigenschaften auf.

Dezentrale Organisation. Die im Grid verbundenen Ressourcen können sich über viele juristisch, organisatorisch und administrativ autonome und geografisch verteilte Unternehmen erstrecken. Grids unterliegen generell keiner zentralen Kontrolle.

Diese Anforderung widerspricht jedoch in keiner Weise der Anforderung mit der Ordnungsnummer 8 aus Abschnitt 3.1.4 („Etablierung einer vertrauenswürdigen Koordinationseinheit im GIDS“), die, wie in den weiteren Ausführungen beschrieben, auch als zentrale Anlaufstelle für die Koordination (in Anlehnung an beispielsweise ein GOC) eines GIDS dient. Auch der Aktor „Betreiber des GIDS“ (siehe auch Tabelle 3.6 auf Seite 23) steht hiermit nicht im Konflikt. Dieser ist insbesondere gefordert, da potentiell auch zum Beispiel Virtuelle Organisationen, die keine eigene Instanz des GIDS betreiben wollen, durchaus zum Kundenkreis eines solchen Systems zählen können. Dies impliziert nicht, dass eine zentrale Organisation vorliegt, da durchaus weitere Instanzen, wie in den nachfolgenden Kapiteln genauer erläutert, untereinander kooperieren.

Heterogenität. Als Folge der dezentralen Organisation sind Grids oftmals sehr heterogen aufgebaut. Die eingebrachten Ressourcen können sich stark in Hardware, Software und Netzanbindung unterscheiden.

Diese Tatsache wird auch nochmals an dem gewählten Szenario des D-Grids (siehe Abschnitt 3.1.1) und den daraus abgeleiteten Anwendungsfällen deutlich. Der Umgang mit der Heterogenität auf mehreren Ebenen (verschiedene Grid-Middlewares, unterschiedliche Sicherheitsmechanismen und -vorkehrungen der Teilnehmer etc.) scheint folglich essentiell.

Verwendung standardisierter und offener Protokolle. Nur die Nutzung standardisierter, offener und breit unterstützter Protokolle sowie Schnittstellen als Basis von Grid-Technologien stellt die Interoperabilität innerhalb von komplexen, verteilten Strukturen nachhaltig sicher. Dies dient letztlich auch der Vermeidung von Abhängigkeiten.

Auch diese Tatsache ist bereits in der vorstehenden Anwendungsfall-getriebenen Anforderungsanalyse mehrfach zu Tage getreten. Da für diese Arbeit unter anderem die Idee der kooperativen Nutzung von Sicherheitssystemen zur Formierung eines Grid-weiten Frühwarnsystems steht, bedarf es insbesondere der Verwendung standardisierter und offener Protokolle, um letztlich eine möglichst unkomplizierte Integration unterschiedlicher Systeme zu gewährleisten.

Hohe Leistungsfähigkeit. Der koordinierte Zugriff auf integrierte Ressourcen innerhalb von Grid-Verbünden soll zu einem im Vergleich zur Summe der Einzelsysteme signifikant größeren Nutzen und erhöhter Qualität des Gesamtsystems führen.

Weiter sind durch Grid-Strukturen noch einige generische Anforderungen bedingt, denen sich ein jedes neues System im Grid, also insbesondere auch ein Grid-basiertes Frühwarnsystem, stellen muss.

Skalierbarkeit. Nicht zuletzt durch die hohe Leistungsfähigkeit des Grids bedingt muss auch ein GIDS möglichst ressourcenschonend agieren und somit eine gute Skalierbarkeit gewährleisten. Dabei gilt es ein vermeintlich hohes Informationsaufkommen effizient zu verarbeiten und die Ressourcen im Grid nicht dafür zu verschwenden, sich selbst zu schützen, sondern eine minimale Auswirkung auf die Performanz des Grids zu erzielen (im Englischen auch mit *Low Intrusiveness* bezeichnet).

Nutzung bestehender Grid-Dienste und Einbettung in diese. Die möglichst nahtlose Integration eines Frühwarnsystems in Grid-Umgebungen fördert unter anderem auch die (Nutzer-)Akzeptanz des neuen Systems. Dazu ist die Nutzung bereits existierender Grid-Dienste und die Einbettung in die bestehende Grid-Landschaft notwendig. Diese Anforderungen in spezielleren und somit weniger generischen Ausprägungen spiegeln sich auch schon in der Anwendungsfall-getriebenen Anforderungsanalyse in Abschnitt 3.1 wider, zum Beispiel durch die Anforderung „Einbindung bestehender AA-Mechanismen“ mit der Ordnungsnummer 4 aus Abschnitt 3.1.4.

Dynamik der Ressourcen. In Grid-Umgebungen ist es durchaus üblich, dass die Verfügbarkeit von Ressourcen sich dynamisch ändert. Dabei können entweder neue Ressourcen und Dienste in das Grid eingebracht oder aus dem Grid entfernt werden. In zweiterem Fall ist insbesondere in Bezug auf Frühwarnsysteme zu unterscheiden, ob ein Entfernen einer Grid-Ressource durch eine Störung oder einen erfolgreich durchgeführten Angriff bedingt ist oder ob dies bewusst und gewollt geschehen ist.

Durch diese Dynamik der Ressourcen bedingt folgt direkt eine immense Herausforderung, der ein Grid-weites Frühwarnsystem begegnen muss. Mit dem Hinzukommen und Wegfallen von Ressourcen (ob gewollt oder ungewollt spielt hier keine Rolle) ändert sich die Qualität und Quantität an Information, die dem GIDS zur Analyse bereitsteht. Es gilt auf der einen Seite damit überhaupt umgehen zu können und auf der anderen Seite die Information möglichst korrekt zu interpretieren, so dass keine unnötigen falsch positiven und falsch negativen (*False Positives* und *False Negatives*) Meldungen erzeugt werden beziehungsweise deren Rate minimiert wird.

Dynamik der Nutzer und VOs. VOs und deren Teilnehmer unterliegen einer hohen Dynamik. Da diese durchaus zu dem Nutzerkreis eines GIDS gehören können, gilt es auch dieser Tatsache Rechnung zu tragen. Insbesondere bedeutet dies, dass eine Integration eines Grid-basierten Frühwarnsystems in die VO-Management Werkzeuge und Tools vorgenommen werden muss. Unter Beachtung der zuvor genannten Anforderung der Nutzung von und Einbettung in bestehende Grid-Dienste kann diesem Tatbestand also bereits begegnet werden, da in hiesigem Fall die Anforderungen, die durch die Dynamik der Nutzer und VOs resultieren, eine Teilmenge der bereits angeführten Anforderungen sind.

Erweiterbarkeit und Flexibilität. Aspekte der Dynamik auf den verschiedensten Ebenen erheben vor allem auch die Anforderung, ein jedes Grid-System möglichst gut und einfach erweitern zu können und maximal flexibel gegenüber neuen Komponenten und Teilnehmern zu sein. Spezialfälle dieser pauschalen Anforderung finden sich auch bereits in der Anwendungsfall-getriebenen Anforderungsanalyse in Abschnitt 3.1 wieder. Ein Beispiel dafür ist die Anforderung des „Einbringen[s] zusätzlicher Informationsquellen in das GIDS während des Betriebs“ mit der Ordnungsnummer 5 in Abschnitt 3.1.4.

3.2.2 Mögliche Kooperationsmuster bei GIDS

Bereits einleitend ist die Idee aufgekommen, ein Grid-basiertes Frühwarnsystem als kooperatives System, an dem die einzelnen Teilnehmer des Grids partizipieren, zu gestalten. Dazu sollen insbesondere bestehende Informationsquellen der am GIDS beteiligten Parteien föderiert werden.

Es stellt sich sodann jedoch die Frage nach einem möglichen Kooperationsmuster für einen solchen Zusammenschluss. Grundlegend sind drei Arten der Kooperation denkbar, die in diversen Abwandlungen ausgeprägt sein können:

- keine Kooperation
- hierarchisch organisierte Kooperation
- Peer-to-Peer (P2P)

Eine extreme Form ist überhaupt keine Kooperation einzugehen. Dies widerspricht jedoch dem Ansatz dieser Arbeit, und somit wird dieser Fall nicht weiter betrachtet.

Eine weitere Möglichkeit besteht darin eine streng hierarchische Organisationsform zu wählen. Dies widerspricht jedoch unter anderem der in Abschnitt 3.2.1 geforderten Eigenschaft der dezentralen Organisation eines Grid-Systems, wodurch zumindest eine strenge Hierarchie ausfällt.

Ein Peer-to-Peer Ansatz scheint als Alternative in Frage zu kommen, um insbesondere voranstehenden Anforderungen nachkommen zu können. Insbesondere kann hierdurch eine dezentrale Organisation bei erhöhter Ausfallsicherheit erreicht werden.

Ob eine strenge Einhaltung eines der vorgenannten Paradigmen notwendig ist, wird im Projektverlauf deutlich werden. Es ist durchaus denkbar die positiven Eigenschaften mehrerer Ansätze miteinander zu kombinieren um eine geeignete Organisationsform für den hiesigen Fall zu erzielen. Solche Mischformen finden sich häufig auch in Forschung und produktiven Einsätzen wieder, wie auch in Kapitel 5 zu themenverwandten Ansätzen und Arbeiten nochmals deutlich wird.

3.2.3 Diskussion der Vertrauensbeziehungen

Um eine Kooperation unterschiedlicher Organisationen in einem beliebigen System auf Grundlage eines Informations- und Datenaustauschs gewährleisten zu können, muss eine Vertrauensbeziehung unter den Informationsanbietern bestehen. Dabei sind prinzipiell drei unterschiedliche Grade des Vertrauens festzustellen:

- kein Vertrauen
- eingeschränktes Vertrauen
- uneingeschränktes Vertrauen

Eine extreme Form einer Vertrauensbeziehung stellt die Tatsache dar, gar kein Vertrauen zu einem anderen Informationsanbieter zu haben. In Extremfällen kann dies implizieren, dass keine Informationen ausgetauscht werden und somit folglich auch keine Kooperation, wie in Abschnitt 3.2.2 beschrieben, stattfindet.

Das andere Extrem ist der Tatbestand des uneingeschränkten Vertrauens. Dies bedeutet, dass **alle** Informationen, wie sie bei den jeweiligen Informationsanbietern vorliegen, ungefiltert und nicht verfälscht weitergereicht werden. Diese Situation ist jedoch sehr unwahrscheinlich, da in der Realität zum Beispiel juristische Randbedingungen wie der Datenschutz einen solchen Informationsfluss unterbinden. Auch bei Kooperationen unter konkurrierenden Organisationen ist ein uneingeschränkter Datenaustausch eher unwahrscheinlich.

Aus voranstehend genannten Gründen folgt also die Anforderung an ein GIDS, mit eingeschränkten Vertrauensbeziehungen unterhalb der Kooperationspartner umgehen zu können. Bei korrekter Modellierung können dadurch ebenfalls die beiden Extremfälle, kein beziehungsweise uneingeschränktes Vertrauen zu anderen Kooperationspartnern zu haben, abgedeckt werden. Ersteres entspricht nichts anderem als einer Informationstransformation in Form einer Nullfunktion[2] (alle Informationen werden verworfen), der zweite Fall der einer Identitätsabbildung (alle Informationen werden unverändert weitergeleitet).

An dieser Stelle soll sich nicht weiter mit dem Management von Vertrauensbeziehungen (*Trust Management*) befasst werden. Vielmehr ist diese Disziplin eine Notwendigkeit, um ein kooperatives Grid-basiertes Frühwarnsystem erfolgreich zu etablieren. Bei der weiteren Konzeption eines solchen müssen die Möglichkeiten, Trust Management-Aspekte um- und durchzusetzen, vorgesehen werden. Dabei ist insbesondere zu beachten, dass Vertrauensbeziehungen

[2]Sei $f : A \to B$. Wenn gilt, dass $f(x) = 0$ für alle $x \in A$, so ist f eine *Nullfunktion*.

in den wenigsten Fällen als ein einziger globaler Wert ausgedrückt werden können, sondern zumeist paarweise unterschiedliche Vertrauensbeziehungen zwischen den Teilnehmern (hier an einem GIDS) bestehen.

3.3 Kriterienkatalog für die Auswahl von IDS für Grids

Zusammenfassend ergibt sich aus voranstehenden Kapiteln nun ein Katalog an Anforderungen an ein IDS im Umfeld von Grids, der zur Bewertung und Auswahl eines IDS für Grids dienen kann. Zur Strukturierung der Anforderungen bietet sich eine Unterteilung in funktionale und nichtfunktionale Anforderungen, Sicherheitsanforderungen, organisatorische und Datenschutzanforderungen sowie Anforderungen an die Erkennungsleistung des IDS an.

Funktionale Anforderungen. Die funktionalen Anforderungen, die spezielle Funtionalitäten eines Systems spezifizieren, zerfallen in drei weitere Klassen. Zuerst finden sich eine Reihe Anforderungen, die generisch für jedes Intrusion Detection System scheinen, egal in welcher Umgebung es eingesetzt werden soll. Hinzu ergeben sich jedoch zwei weitere Klassen. Zum einen lassen sich ein Teil der funktionalen Anforderungen auf den Einsatzzweck des IDS in einer verteilten, föderierten Umgebung zurückführen. Diese sind zwar nicht primär durch Grids bedingt, sind aber dennoch insbesondere in Grids wie in anderen verteilten Systemen anzutreffen. Zudem lässt sich eine dritte Klasse der eindeutig durch Grids bedingten Anforderungen aufstellen. Die hierunter fallenden Anforderungen beziehen sich vorwiegend auf die Integration eines GIDS in die bestehenden Grid-Dienste sowie das eigene Bereitstellen eines neuen Grid-Dienstes.

Nichtfunktionale Anforderungen. Ähnlich wie bei den funktionalen Anforderungen lassen sich die nichtfunktionalen Anforderungen, die eine Eigenschaft eines Systems spezifizieren, in drei Unterklassen einteilen. Auch hier lässt sich die Unterteilung in die generischen, die unter anderem auch durch Grid bedingte sowie die eindeutig durch Grids bedingten Anforderungen vornehmen.

Sicherheitsanforderungen. In [38] werden Sicherheitsanforderungen eigentlich als eine Unterklasse der nichtfunktionalen Anforderungen gesehen. Da im Rahmen dieser Arbeit jedoch ein System zur Durchsetzung von Sicherheitsanforderungen konzipiert wird, sollen die Sicherheitsanforderungen an dieses System gesondert hervorgehoben werden.

Aus den voranstehenden Teilabschnitten dieses Kapitels sind in Bezug auf die Sicherheit maßgeblich zwei Klassen von Anforderungen hervorgegangen. Zum einen sind dies Anforderungen an die Sicherheit der Kommunikation innerhalb und mit dem System, zum anderen werden Eigenschaften zur Nutzerverwaltung, also insbesondere der Authentifizierung und Autorisierung von Nutzern, gefordert.

Organisatorische und Datenschutzanforderungen. Durch eine Reihe von Randbedingungen unterliegt auch ein Grid-basiertes Intrusion Detection System organisatorischen und Datenschutzanforderungen. Auch diese Klasse von Anforderungen ist nach [38] im eigentlichen Sinne eine Unterklasse der nichtfunktionalen Anforderungen. Es lässt sich dabei feststellen, dass eine Unterteilung zum einen in die eher prozessorientierten, organisatorischen Anforderungen eignet, eine zweite Unterklasse an Anforderungen bilden zumeist durch juristische Randbedingungen sowie Datenschutzanforderungen gegebene Notwendigkeiten ab.

Anforderungen an die Erkennungsleistung. Anforderungen, die sich an die Erkennungsleistung eines Grid-basierten Frühwarnsystems stellen, finden sich naturgemäß analog in herkömmlichen IDS wieder. Eine gewisse Ordnung dieser Klasse an Anforderungen lässt sich auch hier vornehmen, so existieren zum einen Anforderungen, die sich an örtlichen Aspekten orientieren, zudem gilt es auch unterschiedliche Angriffstypen und -muster erkennen zu können. Also ergeben sich zum anderen Anforderungen bezüglich der Art und Dauer eines Angriffs.

Es ist zu beachten, dass die in diesem Kapitel erhobenen Anforderungen aus den Lebenszyklusphasen des Aufbaus und Betriebs eines Grid-basierten Frühwarnsystems entstammen. Es wird antizipiert, dass ein einmal etabliertes GIDS über die gesamte Zeitspanne des Betriebs des zu schützenden Grids existent bleibt und erst mit Beendigung der Grid-Infrastruktur ebenfalls terminiert wird. Ein entsprechender Prozess bleibt zu spezifizieren, dieser ist jedoch nicht Bestandteil dieser Arbeit. Dies bedeutet jedoch nicht, dass nachfolgende Anforderungen Änderungen am Frühwarnsystem (zum Beispiel Hinzufügen und Entfernen von Grid-Sites oder Sensorik) zur Laufzeit ignorieren. Lediglich die Außerbetriebnahme des Gesamtsystems findet hier keine Beachtung.

Tabelle 3.20 stellt nochmals übersichtlich alle in diesem Kapitel erhobenen Anforderungen an ein Grid-basiertes Intrusion Detection System dar. Die Anordnung der Anforderungen folgt zuvorstehender Kategorisierung.

funktionale Anforderungen	Unterstützung verschiedener Granularitätsstufen bei der Berichterstattung	
	Berichterstattung zu qualitativ differierenden Angriffen	
	Aussagekräftige Informationsaufbereitung	
	Zugriffsmöglichkeit auf Sensordaten	
	Variationsmöglichkeit der Informationsquellen/Datenbasis zur Laufzeit	
	Proaktive Benachrichtigung der Kunden	
	unter anderem auch Grid-bedingt	Nutzung verschiedener Kommunikationsmodelle (Push, Pull, Stream)
		Aggregatbildung
	Grid-bedingt	Informationspräsentation im Grid-Portal
		Nutzung bestehender Grid-Dienste
		Anbindung an bzw. Nutzung von bestehenden VO-Managementsystemen
nichtfunktionale Anforderungen	Integrierbarkeit in bestehende Management-Werkzeuge	
	Interoperabilität	
	Mandantenfähigkeit	
	Nachvollziehbarkeit durchgeführter Anfragen	
	Portabilität	
	Wiederverwendbarkeit	
	unter anderem auch Grid-bedingt	Dezentrale Organisation
		Einheitliche Schnittstellen
		Erweiterbarkeit und Flexibilität
		Hohe Leistungsfähigkeit
		Skalierbarkeit
	Grid-bedingt	Dynamik der Nutzer und VOs
		Dynamik der Ressourcen
		Unterstützung etablierter (Grid-) Standards
		Unterstützung Virtueller Organisationen
Sicherheitsanforderungen	Kryptographische Anforderungen	Vertraulichkeit von Daten und Nachrichten
		Authentizität von Daten und Nachrichten
		Integrität von Daten und Nachrichten
		Einsatz symmetrischer und/oder asymmetrischer Kryptografie
		Kanal- oder nachrichtenbasierte Kommunikationssicherung
	Nutzerverwaltung	Integration in PKI
		Delegation von Identitäts- und Berechtigungsnachweisen
		Single Sign-On mit Proxy-Zertifikaten
		Einbindung bestehender AA-Mechanismen

		Zugriffsbeschränkung auf Informationen
Organisatorische und Datenschutzanforderungen	Organisatorische Anforderungen	Etablierung einer vertrauenswürdigen Koordinationseinheit
		Prozessspezifikation für (Signatur-) Updates
		Gewährleistung der Autonomie beteiligter Informationsanbieter
	Datenschutz	Anonymisierungs- und/oder Pseudonymisierungsmöglichkeiten
		Durchsetzung des Datenschutzes
		Nachhalten historischer Berichte
		Archivierung von Sensordaten
Erkennungsleistung	Örtliche Aspekte	Schutz der potentiellen Angriffsziele
		Geeignete Sensorplatzierung
	Angriffstypen und -muster	Erkennung verschiedener Angriffstypen (aktiv, passiv/autonom, DoS)
		Entdecken kurzzeitig angelegter bis hin zu zeitlich lang andauernden Angriffe

Tabelle 3.20: Zusammenfassung der erhobenen Anforderungen

Kapitel 4

Bedrohungsanalyse

4.1 Einleitung

Beim Design eines Intrusion Detection Systems (IDS) ist es von entscheidender Bedeutung, die Ausgangslage zu kennen und Ziele präzise festzulegen. Ziel jedes IDS ist die Erkennung und gegebenenfalls Bewertung von Angriffen. Die Reaktion auf den Angriff baut auf den Informationen der Angriffserkennung auf:

- Ist der Angriff erfolgreich?
- Welche Ziele verfolgt der Angriff?
- Welchen Umfang hat der Angriff?
- Woher stammt der Angriff?
- Welchen Schaden hat der Angriff verursacht?

Für ein komplexes System wie ein Grid kann davon ausgegangen werden, dass mehrere Sensoren zur Angriffserkennung zu einem System kombiniert werden müssen. Dies ist insbesondere auch deshalb notwendig, weil viele Angriffe mehrere Subziele verfolgen. So kann ein Angreifer beispielsweise die Identität eines Benutzers übernehmen, um dann im zweiten Schritt die Kontrolle über andere Systeme im Grid zu übernehmen. In diesem Fall ist es wichtig, den vollständigen Umfang des Angriffs möglichst frühzeitig zu erkennen.

Die Anforderungen an ein Grid-IDS gehen aus den bekannten und aktuellen Bedrohungen hervor, denen das Grid ausgesetzt ist. Für eine Übersicht über die Bedrohungen werden verschiedene Quellen herangezogen. Das sind öffentliche Informationen von AV-Herstellern, Daten von Internet-Frühwarnsystemen und Erfahrungen des DFN-CERTs.

4.1.1 Gliederung der Bedrohungsanalyse

Das Ziel ist, die Bedrohungen für das D-Grid aufzulisten und zu bewerten. Ausgehend davon wird untersucht, in wieweit diese Bedrohungen von der aktuellen Sensorik berücksichtigt werden. Im ersten Abschnitt wird eine Übersicht über die technischen Grundlagen der Sensorik und der Bedrohungsanalyse gegeben, soweit diese für das Verständnis wichtig sind. Danach wird die aktuelle Bedrohungslage zusammengefasst. Den Hauptteil des Kapitels bildet die Beschreibung der ausgewählten Szenarien. Dabei beschreibt jedes Szenario eine Gruppierung von Bedrohungen. Den Abschluss bildet eine Liste der Anforderungen an das Grid-IDS, die aus der Bewertung der Szenarien abgeleitet ist.

4.2 Zusammenfassung der Grundlagen

In diesem Abschnitt wird eine Übersicht über die technischen Grundlagen der Sensorik zur Erkennung von Angriffen im Internet gegeben.

4.2.1 Technische Grundlagen: Sensorik zur Angriffserkennung

Insgesamt stehen die folgenden Klassen von Sensoren zur Verfügung, die auch im Rahmen des Grid-IDS eingesetzt werden können:

Netflow Exporter Netflow ist ein von der Firma Cisco eingeführter Standard, um die Kommunikationsbeziehungen der Systeme in einem Netzwerk aufzuzeichnen. Inzwischen unterstützen alle Hersteller von Routern den Export von Netflows und mit dem RFC 3954 ist ein offener Standard eingeführt worden. Netflow-Daten enthalten:

- **Zeitstempel** für jede Netzwerk-Verbindung.
- **Protokoll-Typ** (z. B. TCP, UDP oder ICMP)
- Die **IP Adressen** für jede Verbindung. UDP-Pakete werden zumeist nach einer Heuristik zu einer Verbindung zusammengefasst.
- Die **Ziel- und Quell-Ports** für die Verbindung.
- **Weitere Informationen**, wie beispielsweise TCP-Flags, TOS-Informationen, Router-Interfaces und Byte- und Paketzähler.

Besonderer Vorteil der Netflows ist die hohe Informationsdichte und die Unabhängigkeit von a-priori Informationen (z.B. Signaturen). Zwar sind die eigentlichen Nutzdaten der Verbindung nicht vorhanden, trotzdem ist häufig eine Rekonstruktion der zeitlichen Abläufe eines Angriffs möglich. Weiterhin lassen sich Anomalien im Netzwerkverkehr leicht finden, wie sie beispielsweise durch Internet-Würmer und andere Malware erzeugt werden.

Signatur-basierte IDS Intrusion Detection Systeme (IDS) überwachen den Datenstrom nach bekannten Angriffsmustern (Signaturen). Dabei können diese sowohl auf Netzwerk-Ebene eingesetzt werden, als auch direkt auf den zu überwachenden Rechner laufen. Vorteil dieser Systeme ist, dass bekannte Angriffe nicht nur erkannt, sondern auch klassifiziert werden. Allerdings lassen sich unbekannte Angriffe nur durch Zufall erkennen.

Anomalie-basierte IDS Signatur-basierten IDS haben den Nachteil, dass für unbekannte Angriffe keine Signaturen zur Verfügung stehen und diese nur durch zufällige Übereinstimmung mit einer Signatur für einen anderen Angriff erkannt werden. Die Annahme von Anomalie-basierten IDS ist, dass ein Angriff zu einer Abweichung des normalen Zustands im Netzwerk führt. Diese Annahme ist speziell plausibel für Internet-Würmer, die zumeist deutliche Charakteristika im Netzwerkverkehr haben. Typische Folge ist ein hoher Anstieg der Netzwerk-Last auf einem einzelnen Port und ein hohes Maß an gescheiterten Verbindungsversuchen. Typischerweise wird der Normalzustand eines Netzwerkes durch ein statistisches Modell beschrieben. Weicht der gemessene Zustand von den Normalzustand ab, wird ein Angriff vermutet. Allerdings sind diese IDS nur dann einsetzbar, wenn ein stabiles Modell für den Normalzustand gefunden werden kann. Im Allgemeinen sind sie anfällig gegenüber Fehlalarmen.

Honeypots Honeypots sind Computersysteme, bei denen Angriffe oder sogar deren Kompromittierung beabsichtigt sind, um vom Verhalten des Angreifers zu lernen. Dabei wird zwischen dem Grad der Interaktion unterschieden. Auf Honeypots mit hohem Interaktionsgrad wird ein vollständig operatives Betriebssystem betrieben. Typischerweise sind die Systeme um vielfältige Funktionen zur Protokollierung der Daten bei Angriffen ausgerüstet. Um einen Missbrauch der Honeypots nach einem erfolgreichen Angriff weitestgehend zu verhindern, werden häufig die Netzwerk-Aktivitäten eingeschränkt. Weiterhin

werden diese häufig in einer virtuellen Maschine betrieben, um den Zustand des Honeypots nach einem Angriff möglichst schnell wieder zu bereinigen. Im Argos Honeypot [36] wird der Monitor der virtuellen Maschine so instrumentiert, dass erfolgreiche Angriffe auf alle Buffer Overflow und verwandte Schwachstellen erkannt werden. Vorteil ist, dass die Analyse des Angriffs unterstützt wird und weiterhin ein Missbrauch des Honeypots zuverlässig verhindert werden kann. Allerdings ist der sehr hohe Verbrauch an Ressourcen und der arbeitsintensive Einsatz von Honeypots mit hohem Interaktionsgrad nachteilig.

Dieses Problem gehen Honeypots mit geringem Interaktionsgrad an. Verwundbare Dienste werden nur grob emuliert. Da dies sehr effizient realisiert werden kann, kann ein einzelnes physikalisches System einen großen Netzwerkbereich überwachen. Weiterhin ermöglicht dieser Ansatz Honeypots wie zum Beispiel Nepenthes [2], Malware zu fangen. Nachteil ist, dass unbekannte Angriffe nicht untersucht werden können und der Honeypot nur mit hohem Aufwand an neue Angriffe angepasst werden kann.

System-Monitoring Jedes Betriebssystem hat Mechanismen, um Status-Informationen (System-Logs) zu speichern. Diese geben einen Überblick über eventuelle Probleme und den Status des Programms oder Ressourcen und Zustände des Betriebssystems. Weiterhin unterstützen viele Betriebssysteme eine umfangreichere Protokollieren der Aktionen von Prozessen und Benutzern.

4.2.2 Grundlagen der Bedrohungsanalyse

Für die Bedrohungsanalyse sind verschiedene Ansätze anwendbar. Ansatzpunkte der Angriffsgraphen und Angriffsbäume ist die mehrstufige Vorgehensweise und die Zielsetzungen bei Angriffen. Dagegen liegt der Schwerpunkte der Taxonomie von Sicherheitsvorfällen und der Bedrohungsmatrix auf der Klassifizierung von Sicherheitsvorfällen und Bedrohungen.

Angriffsgraphen

Angriffsgraphen sind ein formaler Ansatz, der Methoden der Graphentheorie verwendet, um Bedrohungen und Gegenmaßnahmen formal zu beschreiben. Jha et al. definieren in [24] einen Angriffsgraphen G als Tupel von: Zustandsmenge, Menge von Transitionen zwischen Zuständen, Anfangs- und Endzustände und einer Menge von Propositionen, die Aussagen über das System machen. Die Zustände beschreiben den Zustand des Systems zwischen zwei atomaren Angriffen. Die Endzustände sind Ziele des Angreifers, die zum Beispiel die unentdeckte Kompromittierung eines Servers im Netzwerk beinhalten können. Durch den Angriffsgraphen wird formal beschrieben, welche Dienste auf den Systemen laufen, welche Schwachstellen vorhanden sind, ob die Systeme untereinander erreichbar sind und ob Vertrauensbeziehungen zwischen den Systemen existieren. Die während des Angriffs erlangten Privilegien werden als Funktion beschrieben, die für jedes System die Privilegien des Angreifers angibt (keine, Benutzer, Administrator). Ein IDS wird als Funktion von einem Start- und Zielsystem und einem gegebenen Angriff modelliert, die beschreibt, ob der entsprechende Angriff erkannt wird.

Der Angriffsgraph wird für ein Netzwerk auf der Basis der bekannten Topologie, angebotenen Dienste und bekannten Schwachstellen, automatisch aufgebaut. Ist dieser erzeugt, kann mit den bekannten Methoden der Graphentheorie die Sicherheit des Netzwerkes bewertet und wenn notwendig verbessert werden. Dabei wird maschinell überprüft, ob einer der unsicheren Endzustände erreicht werden kann, ohne dass der Angriff durch das IDS erkannt wird. Ist dies der Fall, kann das Modell auf seine Schwachpunkte untersucht und das IDS entsprechend erweitert werden, bis keiner der unsicheren Zustände unentdeckt erreicht wird. Zusammenfassend bieten Angriffsgraphen eine vielversprechende Grundlage für die formale Beschreibung und Bewertung von Bedrohungen für ein bekanntes System. Nachteil ist allerdings der sehr hohe Aufwand für die Erzeugung des Graphen. Weiterhin muss das Netzwerk bis ins Detail formal beschreibbar sein.

Taxonomie von Sicherheitsvorfällen

Eine sinnvolle Vorgehensweise bei der Analyse und Bewertung von Bedrohungen ist es, diese im ersten Schritt zu Klassen zusammenzufassen. Für Sicherheitsvorfälle bei Computersystemen ist eine Klassifizierung durch Howard et al. in [19] vorgenommen worden. Da jeder Vorfall aus einer Bedrohungssituation hervorgeht, bietet diese auch eine Basis für die Klassifizierung von Bedrohungen.

Während des Betriebs von Computern ändert sich der Status von Programmen und Systemzuständen ständig. Beispielsweise meldet sich ein Benutzer beim System an und erhält Zugriff. Vorausgehend ist eine Aktion des Benutzers zur Authentifizierung beim System notwendig. Die Änderung des Zustands beinhaltet eine Aktion und ein Ziel, wobei im obigen Beispiel die Aktion die Authentifizierung des Benutzers und das Ziel der Zugriff auf den Benutzer-Account ist. In [19] wird ein Paar aus Aktion und Ziel als „Event“ bezeichnet. Für eine Klassifizierung von Sicherheitsvorfällen werden speziell die Aktionen betrachtet, die ein Angreifer im Rahmen eines Angriff durchführen kann. Diese beinhalten beispielsweise das Umgehen von Sicherheitsvorkehrungen, Fälschen von Informationen und Stehlen von Passwörtern. Ziele in [19] umfassen Accounts, Prozesse, Daten und Netzwerk-Ressourcen.

Ein Angriff wird als Kombination bestehend aus Angriffswerkzeug, Schwachstelle, Event und Resultat des Angriffs bezeichnet. Dabei umfassen Angriffswerkzeuge nicht nur die bekannten Exploit-Programme, sondern beispielsweise auch mit anderen Angreifern ausgetauschte Informationen oder die Möglichkeit, Informationen auszuspähen (social engineering). Zweck des Werkzeuges ist das Ausnutzen einer Schwachstelle. Dieser Vorgang führt zu einem Event; dies kann das nicht autorisierte Anmelden als Benutzer am Computer sein. Als Folge davon kann der Angreifer nicht autorisierte Aktionen durchführen. Dazu gehört der Zugriff auf vertrauliche Informationen oder die Erweiterung der bereits vorhandenen Privilegien im System. Howard et al. bezeichnen als Sicherheitsvorfall einen um die Komponenten „Angreifer“ und „Angriffsmotivation“ erweiterten Angriff. Dabei werden Angreifer beispielsweise in Hacker, Terroristen, Kriminelle und andere Gruppierungen unterteilt. Zielsetzungen beinhalten das Anrichten von Schaden (Denial of Service) oder einen finanziellen Gewinn. Zusammengefasst besteht ein Sicherheitsvorfall aus den Komponenten:

- Angreifer
- Angriffswerkzeug
- Schwachstelle
- Aktion
- Ziel
- Resultat
- Angriffsmotivation

Aus dieser Taxonomie können Bedrohungen durch Kombination der verschiedenen Werte der Komponenten und Zusammenfassung zu Klassen abgeleitet werden. So läßt sich beispielsweise ein erfolgreicher Angriff auf einen Apache Web-Server durch die Menge beschreiben: („Hacker“, „Exploit-Programm“, „Buffer Overflow im Apache Webserver“, „Übernehmen“, „Prozess (Apache)“, „nicht autorisierter Zugang zu Ressourcen“ und „Finanzieller Gewinn“. Diese kann dann verallgemeinert werden: „Ein Angreifer kompromittiert einen Webserver, um ihn für kriminelle Zwecke zu missbrauchen.“

Bedrohungsmatrix

In [9] wird eine Bedrohungsmatrix als zweidimensionale Tabelle definiert, die aus Gefährdungsbereichen und Auslöser der Bedrohungen besteht. Gefährdungsbereiche werden in interne Angriffe, externe Angriffe, Denial of Service und andere Klassen aufgeteilt. Auslöser umfassen

interne und externe Benutzer, mobiler Code und Programmierer. Ein Vergleich mit der Taxonomie von Sicherheitsvorfällen zeigt, dass die Matrix auf einer sehr ähnlichen Idee basiert. Jedoch umfasst die Taxonomie deutlich mehr Kriterien im Vergleich zur Bedrohungsmatrix.

Bedrohungsbaum

Ein Bedrohungsbaum dient dazu, die Bedrohung für ein ausgewähltes Szenario zu beschreiben. Die Wurzel des Baums ist ein Ziel des Angreifers. Dies kann beispielsweise die Impersonifizierung eines anderen Benutzers auf einem bestimmten System sein. In dem Angriffsbaum werden dann alle Wege beschrieben, auf denen der Angreifer sein Ziel erreichen kann. Dies können mehrere alternative Wege sein, wobei jeder individuell zum Ziel führt. Weiterhin beinhaltet jeder Pfad Subziele, die letztendlich zum Erreichen des Ziels notwendig sind. Subziele können beispielsweise das erfolgreiche Anmelden unter dem Namen des Benutzers sein. Dies kann als weitere Subziele entweder das Umgehen der Authentifizierung oder Erraten des Passwortes erfordern.

4.2.3 Zusammenfassung und Ausblick

Ziel der Taxonomie von Sicherheitsvorfällen und der Bedrohungsmatrix ist eine Klassifizierung von Bedrohungen. Dafür werden die unterschiedlichen Komponenten der Bedrohungen charakterisiert, die im Fall der Taxonomie unter anderem das Ziel, die Aktion und das erzielte Resultat beinhalten. Durch Kombination der verschiedenen Werte der Komponenten lassen sich so konkrete Bedrohungen ableiten. Allerdings ist die Anzahl der so gewonnenen Bedrohungen zu groß, um alle bewerten zu können.

Bei den Angriffsbäumen und Angriffsgraphen werden mehrere Bedrohungen gruppiert. Eine Gruppe ergibt sich durch den Pfad zum Ziel. Vorteilhaft bei den Angriffsgraphen ist, dass sowohl die Netzwerktopologie berücksichtigt wird als auch die Auswahl und Position der IDS-Sensoren optimiert werden kann. Jedoch müssen die Eigenschaften und Grenzen der Sensoren im Vorfeld eindeutig festgelegt und formal beschrieben werden. Diese ist in der Praxis aber häufig nur sehr eingeschränkt möglich und sehr aufwendig. Als zusätzliches Problem leiden netzwerk-basierte IDS in der Regel unter einer hohen Zahl von Fehlalarmen, die sich nur schwer formal beschreiben lassen. Weiterhin ist der Aufwand erheblich, einen Angriffsgraphen für ein größeres Netzwerk zu konstruieren.

Im weiteren bietet es sich an, die Vorteile aus der Taxonomie von Sicherheitsvorfällen und den Angriffsgraphen zu kombinieren. Durch sinnvolles Zusammenfassen von Bedrohungen der Taxonomie bilden sich Gruppierungen, die komplexere *Szenarien* beschreiben. Innerhalb der Szenarien kann eine Struktur geschaffen werden, die aus den Angriffsgraphen entlehnt ist. Um sinnvolle Gruppierungen zu finden, wird im nächsten Abschnitt eine Übersicht über die aktuelle Bedrohungslage im Internet gegeben. Diese Bedrohungen berücksichtigen zwar nicht die Grid-Infrastrukturen, können aber auf diese übertragen werden. So kann davon ausgegangen werden, dass alle aktuellen Angriffe auch Grid-Systeme betreffen. Desweiteren muss davon ausgegangen werden, dass Grids aufgrund ihrer hohen Leistungsfähigkeit in absehbarer Zeit spezielles Ziel von Angriffen werden können. Dies ist auch deshalb absehbar, weil Grids und das verwandte Cloud Computing immer mehr in das Bewusstsein der Öffentlichkeit gelangen.

4.3 Aktuelle Bedrohungslage im Internet

Die allgemeine Bedrohungslage im Internet wird von unterschiedlichen Blickwinkeln durch verschiedene Quellen beschrieben. Zwar bezieht sich keine dieser Quellen speziell auf Grids, jedoch können die Bedrohungen auf Grids übertragen werden. Die Quellen umfassen Informationen von Herstellern von Antiviren-Produkten (AV), aus Internet-Frühwarnsystemen und den Erfahrungen von Computer Emergency Response Teams (CERTs). Im folgenden Abschnitt werden die Informationen dieser Quellen zusammengefasst.

4.3.1 Schwachstellen und Malware

Eine gute und umfangreiche Übersicht über die Bedrohungssituation für PCs gibt der Bericht von Symantec in [45] aus dem Jahr 2008. Dabei werden Schwachstellen und Sicherheits-Updates nach verschiedenen Aspekten und Kategorien untersucht. Unterschieden wird zwischen Web-Browsern, Client-Anwendungen, Servern und anderen Anwendungen. Analog zu Web-Browsern greifen Client-Anwendungen auf Daten von Diensten im lokalen Netzwerk oder Internet zu. Häufig erfolgt der Zugriff über den Web-Browser, der die Daten an die Client-Anwendung weitergibt. Weiterhin wurden Anwendungen und Betriebsystem-Komponenten hinzugenommen, bei denen sich Schwachstellen nur von am lokalen System angemeldeten Benutzern ausnutzen lassen.

Schwachstellen in Servern sind insbesondere dann kritisch, wenn sie sich ohne vorherige Authentifizierung ausnutzen lassen. Diese Schwachstellen sind speziell für die Integration in Internet-Würmer geeignet, da sich somit der Wurm automatisch verbreiten kann. Schwachstellen in Web-Browsern und Client-Anwendungen benötigen dagegen die aktive Interaktion des Benutzers, typischerweise der Zugriff auf eine Web-Seite oder E-Mail eines Angreifers. Im Gegensatz zu der vorherigen Klasse bieten Firewalls kaum Schutz, weil diese fast immer Web-Anfragen in das Internet zulassen. Weiterhin unterstützen alle Browser kryptographisch gesicherte Protokolle. Dies macht die Erkennung von Angriffen durch netzwerk-basierte IDS unmöglich. Andere Schwachstellen lassen sich nicht direkt über das Netzwerk sondern nur durch einen lokal am Computer angemeldeten Benutzer ausnutzen. Dies sind insbesondere Schwachstellen in lokalen Kommandos oder Anwendungen, die mit erweiterten Rechten laufen. Speziell betroffen sind der Kern des Betriebssystems und unter Unix/Linux SetUID root Befehle. Häufig werden diese Schwachstellen nach einem erfolgreichen Angriff aus dem Netzwerk ausgenutzt, um die Rechte zu erweitern. Diese erweiterten Rechte werden benötigt, um nachfolgend Root-Kits und andere Malware installieren zu können.

Laut des Symantec Berichts in [45] betreffen die überwiegende Anzahl der Schwachstellen[1] in allen Betriebssystemen (berücksichtigt wurden die Hersteller Microsoft, Apple, HP, Sun und Red Hat Linux) Web-Browser und Client-Anwendungen. In Microsoft-Betriebssystemen sind das über 80% in Kontrast zu 14% der Schwachstellen, die Server betreffen. Nur 5% der Schwachstellen betreffen Betriebssystem-Komponenten oder Programme, die in die Klasse der ausschließlich lokal ausnutzbaren fallen. In den anderen Betriebssystemen ist der Anteil der Schwachstellen in Web-Browsern und Client-Anwendungen etwas geringer. Dies läßt sich damit erklären, dass auch viele Produkte von Dritt-Herstellern und aus der Open-Source Community berücksichtigt wurden. Das heißt, der Anteil der Client-Anwendungen und Browser-Komponenten ist insgesamt geringer als in Microsoft-Betriebssystemen. Dies wirkt sich auch auf den prozentualen Anteil der Schwachstellen in diesen Komponenten aus. Unabhängig vom Betriebssystem liegt der Anteil an Schwachstellen in Servern zwischen 14 und 19%.

Als weiterer wichtiger Aspekt der Bedrohungssituation wurde in [45] der Zeitraum untersucht, der zwischen der Veröffentlichung von Exploits zum Ausnutzen einer Schwachstelle und der Veröffentlichung des entsprechenden Software-Updates zum Schließen liegt. Dieser Zeitraum ist deshalb kritisch, weil die Software ohne direkten Schutz der Kompromittierung ausgesetzt ist. In [45] wurde dieser Zeitraum speziell für die Browser *Internet Explorer*, *Mozilla*, *Opera* und *Safari* ausgewertet. Dabei wurden für alle Browser durchschnittliche Werte zwischen 3 und 5 Tagen ermittelt, die sich auf das zweite Halbjahr in 2007 beziehen. Mit 11 Tagen wurde für den Internet Explorer in ersten Halbjahr 2007 eine höhere Zeitspanne ermittelt. Der längste Zeitraum für die Entwicklung eines Patches betrug 90 Tage. Allerdings ist unklar, wie kritisch diese Schwachstelle und damit das Security-Update gewesen ist.

Als weiterer Trend wurde im Symantec-Bericht die Anfälligkeit von Web-Anwendungen genannt. Ungefähr 60% der in 2007 veröffentlichten Schwachstellen betrafen diese Anwendungen. Dabei ist zu beachten, dass für diese Anwendungen Sicherheits-Updates nur zu einem sehr kleinen Anteil von den oben genannten Hersteller herausgegeben werden. In der obigen Statistik erscheinen diese Anwendungen deshalb nur zu einem geringen Teil. Insbesondere betroffen sind Anwendungen, die in der Sprache PHP implementiert worden sind. Ein sehr

[1] Berücksichtigt wurden alle Schwachstellen, für die der Hersteller ein Sicherheits-Update herausgegeben hat.

häufig vorkommender und sicherheitskritischer Fehler ist die Verwendung des „include“ oder eines verwandten Kommandos zum Einbinden weiterer lokaler Dateien. Fehler bei Benutzung dieser Kommandos führen dazu, dass ein Angreifer Code von einen anderen Webserver im Rahmen der Anwendung ausführen kann (siehe zum Beispiel [13],[27]). Weiterhin waren und sind fast alle bekannten Web-Anwendungen von Schwachstellen beim Aufruf von Datenbankabfragen (SQL Injection Schwachstellen) und dynamischen Einbinden von Inhalten in HTML-Seiten (Cross-Site-Scripting) betroffen. Mittels SQL Injection kann ein Angreifer beliebige SQL-Kommandos im Rahmen der Datenbank ausführen. Ursache ist der unsichere Umgang mit Variablen, die vom Server dem Skript übergeben werden. Fehler ist das ungeprüfte Einbinden der Inhalte dieser Variablen in ein SQL-Kommando. Da SQL-Kommandos interpretiert werden, kann ein Angreifer durch Einfügen von Sonderzeichen bewirken, dass die Inhalte nicht mehr als Werte sondern als SQL-Schlüsselworte interpretiert werden. Dadurch kann ein Angreifer ohne Autorisierung auf Inhalte der Datenbank zugreifen oder den Server kompromittieren. Cross-Site-Scripting Schwachstellen haben ihre Ursache in dem unsicheren Einbinden von Inhalten in eine dynamisch aufgebaute HTML-Seite. Beispiel hierfür ist eine Suchanfrage, die die angefragten Wörter in eine dynamisch erzeugte Seite einfügt. Analog zu SQL Injection ist die Fehlerursache das ungeprüfte Einbinden von Inhalten in die dynamisch erzeugt HTML-Seite. Dadurch kann ein Angreifer erreichen, dass die eingefügten Inhalte als HTML Schlüsselworte im Web-Browser des Benutzers interpretiert werden. Häufig werden die Auswirkungen von Cross-Site-Scripting Schwachstellen als weniger kritisch angesehen. Jedoch werden häufig Cookies auch von sicherheitskritischen Web-Anwendungen verwendet, über die sich ein Benutzer bei einer Web-Anwendung authentifiziert. In diesem Fall kann das Cookie durch Cross-Site-Scripting vom Angreifer geklaut und zur Übernahme der Identität des Benutzers missbraucht werden. Weiterhin schützen kryptographische Protokolle, wie beispielsweise HTTPS, nicht vor dem Ausnutzen von Cross-Site-Scripting- und SQL-Injection-Schwachstellen.

Allgemein läßt sich die sehr hohe Anzahl an Schwachstellen in Web-Anwendungen damit erklären, dass diese auf der einen Seite von Laien sehr leicht durch die Skript-Sprachen erstellt werden können. Auf der anderen Seite setzt die sichere Erstellung eine umfangreiche Erfahrung voraus, wodurch die Mehrzahl der Anwendungen von leicht zu erkennenden Schwachstellen betroffen war. Dies zeigt sich auch sehr deutlich an der hohen Anzahl an veröffentlichten Exploit-Programmen beispielsweise auf der Seite von Milw0rm [33].

4.3.2 IT-Frühwarnsysteme

Eine weitere wichtige Quelle für die Bewertung von Bedrohungen sind IT-Frühwarnsysteme. Ziel dieser Systeme ist das Sammeln von Informationen und die Überwachung der Angriffs-Aktivitäten im Internet. Die Quellen umfassen dabei Informationen, die aus Mailing-Listen, Informationen von AV-Hersteller und Informationen von Computer Notfall-Teams (CERTs) gewonnen werden. Die Informationen können sowohl aus öffentlichen als auch aus nur eingeschränkten Benutzerkreis angebotenen Quellen stammen. Vorteil öffentlicher Quellen ist, dass keine Vereinbarung über die Vertraulichkeit und Weitergabe von Daten berücksichtigt werden müssen. Allerdings sind diese Quellen häufig weniger vertrauenswürdig, was insbesondere auf öffentliche Mailing-Listen zutrifft.

Angriffs-Informationen werden durch Sensoren aufgezeichnet, die entweder in produktiven oder unbenutzten Netzwerken eingesetzt werden. Diese umfassen alle der in Abschnitt 4.2.1 genannten Sensoren. Da die überwiegende Anzahl der Angriffe im Internet ungezielt ist, reicht es für statistische Informationen aus, Sensoren in unbenutzten Netzwerken einzusetzen. Weitere Vorteile sind, dass es in diesen Netzwerken keinen legitimen Netzwerkverkehr gibt und die aufgezeichneten Daten bezüglich des Datenschutzes als unproblematisch gesehen werden können. Allerdings lassen sich Angriffe innerhalb eines produktiven Netzwerkes nur erkennen, wenn die Sensoren in dem Netzwerk positioniert sind. Da auch legitimer Netzwerkverkehr vorhanden ist, besteht die spezielle Herausforderung, zwischen diesem und Angriffen zu unterschieden. Weiterhin werden mit hoher Wahrscheinlichkeit personenbezogene Daten aufgezeichnet, die entsprechend geschützt werden müssen.

Ein aktuelles Frühwarnsystem mit dem Schwerpunkt auf einen produktiven Betrieb ist durch das CarmentiS Projekt [1] entwickelt worden. CarmentiS ist ein Gemeinschaftsprojekt von Sicherheitsteams des deutschen CERT-Verbunds in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI). Die Daten werden von verschiedenen Sensoren aufgezeichnet, die im Netzwerk von *Datenzulieferern* betrieben werden. Die Sensoren umfassen IDS, Honeypot-Daten und Netflow-Exporter. Alle Daten laufen zentral in der *Datenzentrale* ein und werden dort auf einer grafischen Oberfläche dargestellt. Dabei wurde ein Schwerpunkt beim Konzept auf die Aggregation und Korrelation von Daten aus unterschiedlichen Quellen gelegt. Diese ermöglichen es, wichtige Informationen aus der umfangreichen Datenmenge abzuleiten und in kompakter Form zu präsentieren, das heißt, den *Analysten* wird die Interpretation der Daten deutlich erleichtert. Weiterhin unterstützt die grafische Oberfläche die Filterung der Daten nach verschiedenen Kriterien.

CarmentiS ermöglicht eine sehr präzise Überwachung des Hintergrundrauschens im Internet. Das Hintergrundrauschen umfasst alle ungezielten Angriffe, die beispielsweise von Würmern und Bot-Netzwerken ausgehen. Damit lassen sich präzise Statistiken über die Anzahl von kompromittierten Systemen und über Angriffe im Internet anfertigen. Es zeigt sich, dass die Mehrzahl der beobachteten Angriffe im Moment vom W32.Conficker-Wurm ausgehen. Allgemein dominiert die Anzahl der Angriffe auf Windows-Systeme. Allerdings zeigen sich im Hintergrundrauschen auch eine größere Anzahl an Angriffen gegen die TCP-Ports 22 und 21. Aufgrund der Vielzahl an Verbindungen kann auf Angriffe geschlossen werden, die schwache Passwörter bei SSH und FTP zu erraten versuchen.

4.3.3 Aktuelle Sicherheitsvorfälle im Internet und in Grids

Eine Quelle für Tendenzen bei Sicherheitsvorfällen bietet der Symantec Global Internet Security Threat Report in [45]. Als kritische Bedrohung wird in [45] die Kompromittierung personengebundener Daten genannt. Berücksichtigt werden sowohl der Verlust von Daten durch einen Einbruch in ein Computersystem über das Netzwerk als auch durch Diebstahl oder Verlust von Hardware. Quelle ist die DATALOSTdb der Open Security Foundation in [28]. Da die Behandlung personenbezogener Daten ein weitgehendes Vertrauen der verarbeitenden Seite und hohe Sicherheitsanforderungen voraussetzt, ist deren Verlust mit einem hohen Risiko behaftet. Folgen beinhalten einen hohen Schaden in Bezug auf den Ruf und das Vertrauen gegenüber der Einrichtung. Weiterhin kann die Einrichtung für den entstandenen Schaden haftbar gemacht werden. Unter Anderem wird in [45] der Verlust von Daten in den unterschiedlichen Sektoren (akademische Einrichtungen, Regierungseinrichtungen, finanzieller Sektor und Andere) verglichen. Dabei hat sich gezeigt, dass mit 27% akademische Einrichtungen am stärksten betroffen sind, gefolgt von Regierungseinrichtungen mit 20% und der Gesundheitssektor mit 15%. Zwar werden als wichtigste Ursachen der Verlust oder Diebstahl von Hardware genannt (48%) und das Brechen von Policies (21%), allerdings spielt der Einbruch in Computersysteme (Kategorie „Hacking“) mit 17% eine wichtige Rolle.

Die Kompromittierung von Computern ist gegenwärtig zum überwiegenden Teil durch den Missbrauch für kriminelle Tätigkeiten motiviert. So werden diese Systeme zum Versand von Spam-Mails, Durchführung von Angriffen auf Dritte und Diebstahl personenbezogener Daten missbraucht. Beliebtes Ziel sind dabei Heimanwender, die den Computer für Online-Bankgeschäfte verwenden. Die technische Infrastruktur dahinter bilden Bot-Netzwerke. Ein Bot-Netz besteht aus einer Menge kompromittierter Computer auf denen sogenannte Bots installiert sind, die alle von einem Kontrollserver (Command and Control Server) gesteuert werden. Der Bot wird dabei direkt nach der Kompromittierung installiert. Diese kann auf verschiedenen Wegen geschehen: Ein Weg ist der Versand von Malware, die beispielsweise an E-Mails angefügt ist. Weiterhin kann die Malware auf einem Web-Server vorhanden sein und beispielsweise als Anti-Viren Produkt oder Bildschirmschoner getarnt werden. Auf einer Web-Seite wird dann diese Malware beworben. Häufig werden auch Techniken des Social Engineerings angewendet, um den Benutzer zu täuschen. Beispielsweise täuscht eine Web-Seite einen Virenscanner vor, der angeblich vor einer Vielzahl von Viren warnt und ein vermeintliches AV-Programm zum Herunterladen anbietet. Ein weiterer Weg sind Exploit-Pakete, die auf Web-Servern installiert sind. In der Praxis werden dazu auch kompromittierte Web-Server

missbraucht. Ist diese Software auf dem Server installiert, wird jeder Computer automatisch angegriffen, der den Webserver besucht. Da der Browser seine Identität beim Zugriff auf den Webserver preisgibt, kann das Exploit-Programm automatisch einen erfolgversprechenden Angriff auswählen. Nach der Kompromittierung des Computers auf einem dieser Wege wird im zweiten Schritt der Bot nachinstalliert. Dieser baut eine Verbindung zum Command and Control Server auf. Über diesen Server kann ein Angreifer von einer zentralen Position aus alle Bots beziehungsweise die kompromittierten Computer steuern, das heißt, indem der Angreifer einen Befehl über den Server sendet, reagieren alle Bots auf das Kommando. Dies kann zum Beispiel die Installation weiterer Malware oder ein Angriff auf eine dritte Seite sein. Nachinstallierte Malware ermöglicht beispielsweise das Versenden von Spam-Mails. In [45] wird die Anzahl der pro Tag von Symantec beobachteten Bot-infizierten System mit 75 157 genannt. Insgesamt wurden 9 437 536 infizierte System beobachtet.

Vorfälle in Grid-Systemen

Eine gute Übersicht über die aktuelle Situation bei Einbrüchen in Computersysteme haben CERTs (Computer Emergency Response Teams). Eine wichtige Aufgabe dieser Teams ist die Unterstützung der Betroffenen und Reaktion auf gemeldete Sicherheitsprobleme. Beispielsweise betreut das DFN-CERT die am deutschen Forschungsnetz (DFN X-Win) angeschlossenen Universitäten und Forschungseinrichtungen.

Aus den aktuellen Vorfallstatistiken geht hervor, dass neben den Vorfällen durch Windows Malware auch Einbrüche durch Raten oder anderweitige Kompromittierung von Passwörtern eine bedeutende Rolle spielt. So warnt das DFN-CERT beispielsweise in [6] vor der Bedrohung durch Account Probes mit dem Ziel SSH, FTP und andere Passwörter zu raten. Als weitere aktuelle Bedrohungen wird in [6] vor dem Einsatz von Exploits zum Kompromittieren des Linux Kernels und in [51] vor Root-Kits gewarnt. Schwachstellen im Kernel sind insbesondere deshalb kritisch, weil deren Ausnutzung dem Angreifer die vollständige Kontrolle über das System ermöglicht. In der Regel sind diese Schwachstellen allerdings nur von Angreifern ausnutzbar, die über einen gültigen Benutzer-Account verfügen. Deshalb ist deren Ausnutzung nach einem erfolgreichen Angriff üblich, um das System vollständig kontrollieren zu können. Dies ermöglicht die Installation weiterer Malware, wie beispielsweise Root-Kits und Hintertüren im System. Ein Root-Kit dient dazu, vom Angreifer installierte Programme und Prozesse vor den Augen des Administrators zu verbergen. Aktuelle Root-Kits manipulieren in der Regel den Kernel des Systems in einer Weise, dass Prozesse und Dateien des Angreifers nicht mehr durch die Funktionen des Betriebssystems angezeigt werden.

Lokale Root-Exploits und Root-Kits spielten auch in der Vergangenheit bei Vorfällen in Grid-Systemen eine Rolle. In [41] wird die Bedrohung durch Root-Exploits in Grids und deren Gegenmaßnahmen untersucht. Das DFN-CERT und US-CERT berichten in [50] und [49] von einem Vorfall, bei dem in Systeme systematisch mittels kompromittierter SSH-Schlüssel eingebrochen wurde. Dies wurde durch die speziellen Vertrauensbeziehungen zwischen den Systemen möglich. Im Grid-Umfeld ist es typisch, dass Benutzer unabhängig vom Standort auf die Ergebnisse zugreifen können. Dafür erhalten sie einen Zugang über SSH, bei dem sie sich über den privaten SSH-Schlüssel authentifizieren. Dieser ist typischerweise auf dem Computer des Benutzers vorhanden. Durch Kompromittierung des Computers gelangen die Angreifer an den privaten Schlüssel. Als Konsequenz kann mit den gestohlenen Schlüsseln auf alle Systeme zugegriffen werden, auf die der Benutzer Zugriff hatte. Auf diesem Systemen versuchten die Angreifer nach dem initialen Einbruch Root-Rechte durch einen lokalen Angriff auf Schwachstellen im Kernel zu gelangen. War dies möglich, wurde das Root-Kit „Phalanx2“ installiert. Durch Kompromittierung dieser Systeme können eventuell private SSH-Schlüssel anderer Benutzer gestohlen und missbraucht werden.

4.3.4 Zusammenfassung der Bedrohungen

Die wichtigesten Ergebnisse sind zusammengefasst:

- Browser und Client Anwendungen sind sehr unsicher. Schwachstellen lassen sich ausnutzen, um den Benutzer zu überwachen und dessen Identität zu übernehmen.
- Die meisten Angriffe im Internet sind ungezielt und greifen Schwachstellen in Windows Anwendungen an. Beispiel ist der W32.Conficker-Wurm.
- Unter den Diensten dominieren die Schwachstellen in Web-Anwendungen mit deutlichen Abstand. Ursache sind dabei überwiegend Fehler in Skript-Sprachen wie beispielsweise PHP. Diese lassen sich in vielen Fällen (PHP-code Injection oder SQL-Injection) ausnutzen, um die Kontrolle über den Dienst zu übernehmen.
- Schwachstellen im Betriebssystem-Kern lassen sich zwar meistens nur lokal ausnutzen, ermöglichen aber die vollständige Kontrolle über das System. Sie werden typischerweise nach erfolgreichen Angriffen auf Benutzer- oder Dienst-Accounts ausgenutzt, um weitere Malware installieren zu können.
- Bislang wurden nur wenige gezielte Angriffe auf Grids beobachtet. Dabei haben sich allerdings die Beziehungen zwischen den Systemen als verwundbar herausgestellt. Ein Angreifer kann stufenweise verschiedene Systeme im Grid kompromitteren.

4.4 Beschreibung und Bewertung von ausgesuchten Szenarien

In diesem Abschnitt werden die ausgewählten Bedrohungsszenarien vorgestellt und bewertet. Ausgehend von der aktuellen Bedrohungslage und Relevanz für die Grid-Infrastruktur wurden die Szenarien ausgewählt, die für das Grid-IDS von Bedeutung sind.

4.4.1 Zur Rolle der Bedrohungsszenarien

Wie vorher beschrieben, haben die unterschiedlichen Ansätze verschiedene Vor- und Nachteile. Ein pragmatischer Ansatz ist es, aus der Bedrohungsmatrix oder Incident Taxonomy konkrete Szenarien auszuwählen und zu betrachten. Jedes Szenario beschreibt die Bedrohungssituation für das GRID ausgehend von einem oder mehreren ausgewählten Angriffen. Dabei werden die Szenarien betrachtet, die wir aus bekannten Vorfällen und der oben beschriebenen Bedrohungslage für relevant betrachten. Für die Szenarien übernehmen wir die Idee der Angriffsgraphen, dass ein komplexer Angriff aus mehreren aufeinander aufbauenden Angriffen bestehen kann. Diese werden dann in dem Szenario zusammengefasst. Die Kategorien für Szenarien werden folgendermaßen gewählt:

Angriffe: Als Angriff wird hier die aktive Suche oder das Ausnutzen von Schwachstellen verstanden. Die Angriffe können einerseits auf technische Komponenten des Grids abzielen. Diese beinhalten die Server, auf denen die Grid-Middleware läuft, die persönlichen PCs der Benutzer oder die Worker-Nodes. Andererseits können Angriffe direkt auf die gewollte oder ungewollte Kooperation von Benutzern abzielen. Beispielsweise kann mittels Techniken des Social Engineerings versucht werden, deren Passwörter zu erlangen.

Einsatz Malware auf Grid-Systemen: Der Einsatz von Malware hat verschiedenen Ziele. Zuerst werden Exploit-Programme zur Durchführung von Angriffen verwendet. Spezielles Ziel ist es, eine Schwachstelle in der Software auszunutzen, um in ein Computer-System einzubrechen. Da der Einsatz von Exploits Teil eines Angriffs ist, werden diese jedoch in der Kategorie „Angriffe“ behandelt. Häufig werden *Root-Kits* nach einem erfolgreichen Angriff eingesetzt, um die eigenen Spuren auf den kompromittierten System zu verschleiern. Weiterhin ist die Installation von Programmen üblich, um das kompromittierte System über das Netzwerk kontrollieren zu können. Die Erkennung dieser Malware

ist für zwei Zielsetzungen wichtig. Zuerst ermöglicht sie die Erkennung von kompromittierten Systemen, bei denen der initiale Angriff nicht erkannt wurde. Weiterhin ist eine Wiederherstellung des normalen Betriebs nur dann möglich, wenn alle Malware erfolgreich von dem kompromittierten System entfernt wurde.

Missbrauch und Verletzung von Ressourcen: Diese Kategorie behandelt den Missbrauch und die Verletzung der Vertraulichkeit, Integrität und Verfügbarkeit von Ressourcen. Beispiel ist die Ausführung von Programmen zum Kompromittieren von Passwörtern oder um Komponenten des Grids außer Betrieb zu setzen. Eine weitere Möglichkeit des Missbrauchs sind Angriffe auf dritte Seiten, beispielsweise mittels eines verteilten Denial of Service Angriffs. Im Gegensatz zu den vorherigen Kategorien, muss hier nicht zwangsläufig ein Angriff vorausgegangen sein.

Ausnutzung von Schwachstellen: Die Abgrenzung zu den anderen Kategorien ist, dass hier spezielle Kategorien von Schwachstellen behandelt werden. So ist es für die Erkennung von Angriffen wichtig, zwischen bekannten und unbekannten Schwachstellen zu unterscheiden. Die Mehrzahl der Angriffe auf bekannte Schwachstelle wird zuverlässig durch netzwerk-basierte IDS entdeckt. Dagegen schlagen diese Systeme bei Angriffen auf unbekannte Schwachstellen fehl.

Bei der Wahl der Kategorien und Szenarien muss bedacht werden, dass sich diese überschneiden können. Ein Beispiel sind Exploit-Programme zum Ausnutzen von Schwachstellen. Als Szenario läßt sich das sowohl bei den „Angriffen“ als auch bei der „Malware“ einordnen. Allerdings unterscheidet sich die Erkennung von Angriffen deutlich von der Erkennung von Malware, die auf dem lokalen System installiert ist. So produzieren Exploit-Programme häufig charakteristischen Netzwerk-Verkehr, der durch netzwerk-basierte IDS aufgespürt werden kann. Dagegen läßt sich lokal installierte Malware in der Regel zuverlässiger durch AV-Produkte erkennen. Deshalb wird innerhalb der Szenarien zwischen Exploit-Programmen und anderer Malware unterschieden.

Um die Übersichtlichkeit der einzelnen Szenarien zu verbessern, werden diese in mehrere Abschnitte gegliedert. Dabei besteht jedes Szenario aus:

- Einer Einordnung, die aus einer kurzen Beschreibung und Zusammenfassung besteht
- Beschreibung
- Bewertung des Gefahrenpotentials
- Erkennung und Sensorik

Zu jeder der Bedrohungen korrespondieren Angriffe, durch die die Bedrohung ausgelöst wird. In dem Abschnitt „Sensorik zur Erkennung von Angriffen“ werden die technschen Mittel beschrieben, durch die Angriffe erkannt werden können. Diese beinhalten die folgende Sensorik:

- High/Low-interaction Honeypot
- Netzwerk-basiertes IDS
- Host-basiertes IDS (Tripwire) / Virenscanner
- Netflow-Statistiken
- Protokollinformationen der Anwendungen (Logs)

4.4.2 Kategorie Angriffe

Die Szenarien der Kategorie *Angriffe* werden mit A1 bis An durchnummeriert. Diese Nummerierung wird später bei der tabellarischen Auflistung der Szenarien übernommen.

A1 - Kompromittierung von Computersysteme im Grid durch Internet Würmer oder andere automatisierte Angriffe

Einordnung

In dieser Kategorie werden die Angriffe der bekannten autonomen Malware zusammengefasst. Diese umfassen Internet-Würmer wie beispielsweise W32.Conficker und Angriffe von Bot-Netzwerken. Charakteristisch ist, dass diese Angriffe ungezielt auf zufällig ausgewählte Systeme zielen und bekannte Schwachstellen in Diensten versuchen auszunutzen.

Beschreibung

Aus dem Symantec Threat Report in [45] und den Daten vom Internet Frühwarnsystem CarmentiS geht hervor, dass die überwiegende Anzahl an Angriffen im Internet von autonomer Malware ausgeht und ungezielt ist. Ziel der Angreifer ist die Kompromittierung der Systeme, um sie für Angriffe auf andere Systeme und Betrugs-Delikte zu missbrauchen. Häufig werden kompromittierte Systeme in ein Bot-Netzwerk integriert und für Denial of Service oder andere Angriffe missbraucht. Weiterhin wird häufig Malware installiert, die den Benutzer überwacht oder Online-Banking Dienste angreift.

Die größte Bedrohung geht im Moment von dem W32.Conficker-Wurm aus, der sich seit Oktober 2008 im Internet verbreitet. Dieser Wurm nutzt eine Schwachstelle im Windows Server Service (CVE-2008-4250), um in verwundbare Systeme einzubrechen. Varianten, die ab dem 29.12.2008 im Umlauf sind, missbrauchen zusätzlich Wechseldatenträger wie beispielsweise USB-Sticks für die Verbreitung. Ist ein System vom W32.Conficker kompromittiert, beginnt dieses mit der Verbreitung. Dafür werden IP-Adresse ausgewählt, bei denen versucht wird, die Schwachstelle im Server Service auszunutzen. Dazu werden zwei Strategien angewendet. Da mit relativ hoher Wahrscheinlichkeit noch andere verwundbare Systeme in gleichen Netzwerk vorhanden sind, greift der Wurm alle Systeme im gleichen Subnetzwerk an. Weiterhin generiert der Wurm zufällige IP-Adressen, um Systeme in anderen Netzwerken anzugreifen. Neben der Verbreitung über das Netzwerk, schreibt sich der Wurm auf alle Wechseldatenträger, auf die dieser Zugriff hat. Zusätzlich wird eine Datei „autorun.inf“ angelegt, um sich automatisch über das Medium zu starten.

Verläuft der Angriff erfolgreich, wird das Wurm-Programm in Form einer Windows-Bibliothek nachgeladen. Weiterhin verfügt der W32.Conficker-Wurm um zusätzliche Mechanismen, um weitere Malware nachzuladen. Neben Conficker sind aber auch noch viele ältere Internet-Würmer aktiv. Weiterhin beinhalten viele Bot-Netzwerke Kommandos, um Systeme anzugreifen. Dafür gibt der Angreifer einen oder mehrere Exploits und eine Netzwerk-Basisadresse an. Nachfolgend werden dann alle Systeme in diesem Netzwerk-Bereich mittels der gewählten Exploits angegriffen.

Erkennung und Sensorik

Das wesentliche Merkmal dieser Angriffe ist, dass sowohl die ausgenutzten Schwachstellen als auch die Malware an sich bekannt sind. Dies ermöglicht in der Regel die zuverlässige Erkennung durch Netzwerk-basierte IDS. Weiterhin kann davon ausgegangen werden, dass die Wurm-Programme inklusive des W32.Conficker-Wurm zuverlässig durch AV-Programme gefunden werden. Da Internet-Würmer und automatisierte Angriffe ein hohes Maß an Netzwerkverkehr erzeugen, zeigen sie sich in der Regel als Anomalie in den Netflow-Daten. Insbesondere durch Würmer steigt die durchschnittliche Anzahl an Verbindungen ab einem bestimmten Verbreitungsgrad deutlich an.

Bewertung

Zwar sind die Angriffe, die von Internet-Würmern und Bot-Netzwerken ausgehen quantitativ in der Überzahl, jedoch zielen die Angriffe auf bekannte Schwachstellen ab. Ein System, auf dem alle aktuellen Sicherheits-Updates vorhanden sind, ist deshalb nicht anfällig gegen

diese Art von Malware. Allerdings verbreiteten sich viele Würmer zusätzlich noch mit Wechseldatenträger als Medium. Wird beispielsweise ein infizierter USB-Stick innerhalb des Grids ohne die notwendige Sorgfalt verwendet, ist eine Kompromittierung auf diesem Weg möglich. Die besondere Bedrohung ist dabei, dass sich Würmer effektiv innerhalb eines Netzwerkes verbreiten können. Zwar lassen sich alle Würmer effektiv durch IDS und AV-Produkte identifizieren, jedoch hat sich insbesondere beim W32.Conficker-Wurm gezeigt, dass die Säuberung befallener Netzwerke sehr aufwendig ist. Speziell beim Conficker-Wurm sind auch sicherheitskritische Netzwerke kompromittiert worden. Auch aus diesem Grund darf die Bedrohung nicht unterschätzt werden.

A2 - Kompromittierung der Grid-Server/Middleware aus dem Netzwerk

Einordnung

Angriffe können entweder über das Netzwerk oder lokal von einem am System angemeldeten Angreifer erfolgen. Während letztere in dem nachfolgenden Szenario in Abschnitt 4.4.2 behandelt werden, wird hier von einem Angriff über das Netzwerk ausgegangen. Ziel des Angriffs ist es, Schwachstellen in Diensten der Grid-Server/Middleware auszunutzen, zu denen sich der Angreifer verbinden kann. Diese Schwachstellen sind insbesondere dann kritisch, wenn deren Ausnutzung ohne eine vorherige Authentifizierung möglich ist.

Beschreibung

Auch wenn sich die Grid-Toolkits Globus Toolkit, UNICORE und gLITE im Detail unterscheiden, so beinhalten alle gemeinsame Komponenten. Diese gewährleisten die Sicherheit im Grid, Ausführung von verteilten Programmen, Auskunft über Ressourcen des Grids, den Transport und die Speicherung von Daten. Jede dieser Komponenten bietet einem Angreifer Angriffspunkte, über die die Komponenten angegriffen und unter Umständen kompromittiert werden können. Weiterhin existieren zwischen diesen Komponenten verschiedene Vertrauensbeziehungen. Sind die Sicherheits-Dienste kompromittiert, kann ein Angreifer beispielsweise auf beliebige andere Dienste zugreifen. Auf der anderen Seite kann ein Angreifer durch Kompromittierung der Laufzeitumgebung unter Umständen Privilegien erlangen, um die Sicherheits-Dienste zu unterwandern. Im Einzelnen existieren die Komponenten mit den folgenden Angriffspunkten:

Sicherheits-Dienste Über diese Dienste werden Benutzer authentifiziert und es wird die Autorisierung von Aktionen geprüft. Technisch läuft die Authentifizierung von Benutzern über Zertifikate, deren Gültigkeit überprüft wird. Weiterhin existieren Komponenten, die die Privilegien der Benutzer durch Proxy-Zertifikate zu den Komponenten im Grid delegieren. Andere Sicherheitskomponenten gewährleisten den sicheren Transport von Daten im Grid.

Die Sicherheits-Dienste können entweder direkt oder aufgrund von Vertrauensbeziehungen mit anderen Komponenten angegriffen werden. Direkter Angriffspunkt ist die kryptographische Software, die die Grundlage der Dienste bilden. Beispielsweise ist die bekannte Bibliothek *Openssl* von mehreren teilweise schwerwiegenden Problemen betroffen gewesen. Einige führten zu einer Verletzung von Speicherstrukturen (beispielsweise ein Buffer Overflow), die die Ausführung beliebiger Befehle mit den Rechten der Openssl-Anwendung ermöglichte. Ist eine der Grid-Komponenten von dieser oder einer noch nicht bekannten ähnlichen Schwachstelle betroffen, kann ein Angreifer über das Netzwerk den Dienst kompromittieren. Eine noch unbekannte Schwachstelle dieser Art ist zwar nicht sehr wahrscheinlich, kann aber nicht ausgeschlossen werden.

Laufzeitumgebung zur Ausführung von Programmen Die Laufzeitumgebung beinhaltet die Worker-Nodes, Benutzer-Interfaces und einen Scheduler. Über die Interfaces registrieren Benutzer die Abarbeitung von Programmen auf den Worker-Nodes. Der Scheduler legt die Vergabe von Ressourcen fest.

Ein Angriffspunkt sind die Benutzer-Interfaces, die über das Netzwerk erreichbar sind. Ein entfernter Angreifer kann potentiell vorhandene Schwachstellen in den Anwendungen

ausnutzen, um die Kontrolle über die Anwendung zu erlangen. Dabei ist zu beachten, dass insbesondere in Web-Anwendungen in letzter Zeit zahlreiche Schwachstellen gefunden wurden. Zwar unterscheiden sich Web-Services in Grids von diesen Anwendungen. Trotzdem läßt die hohe Komplexität dieser Anwendungen darin enthaltene Schwachstellen vermuten. Weiterhin sind nach unserem Wissen keine umfangreichen Sicherheitstests von Grid-Anwendungen durchgeführt worden.

Informationsdienste für Ressourcen Im einem Grid werden eine Vielzahl von statischen sowie dynamischen Ressourcen verwaltet. Informationsdienste bieten eine Möglichkeit, einen Überblick über diese Ressourcen und deren Auslastung im Grid zu erlangen. Wie bei den Diensten der Laufzeitumgebung sind hier Schwachstellen nicht ausgeschlossen, die ein Angreifer über das Netzwerk ausnutzen kann.

Dienste zum Speichern von Daten In einem Grid fallen viele Daten durch die Benutzer-Programme und deren Verwaltung an. Für deren Speicherung bietet beispielsweise das Globus Toolkit die Dienste GridFTP, RLS und RFT an. Analog zu den anderen Grid-Diensten bieten die Dienste zum Speichern von Daten verschiedene Angriffspunkte. Beispielsweise sind viele bekannte FTP-Server von schwerwiegenden Schwachstelle betroffen gewesen und weitere unbekannte Schwachstellen können nicht ausgeschlossen werden.

Die reale Bedrohung durch die Kompromittierung der Grid-Server/Middleware hängt von der Funktion der Komponente ab. Am kritischsten sind die Dienste für die Authentifizierung von Benutzern. Deren Kompromittierung ermöglicht einem Angreifer die Identität eines beliebigen Benutzers zu übernehmen. Im schlimmsten Fall kann ein Angreifer als Administrator das Grid vollständig unter die eigene Kontrolle bringen.

Die Kompromittierung der anderen Komponenten ist zwar unkritischer. Allerdings ist der Angreifer in der Lage, diese Systeme zu missbrauchen. Beispielsweise kann ein kompromittierter Web-Server zur Kontrolle eines Bot-Netzwerkes oder zum Versand von Spam missbraucht werden. Weiterhin hat ein Angreifer unter Umständen die Möglichkeit, seine Privilegien auf dem kompromittierten System zu erhöhen und Vertrauensbeziehungen zwischen den Systemen zu missbrauchen. Läuft auf dem kompromittierten System ein SSH-Server, der Passwörter akzeptiert, kann ein Angreifer durch dessen Manipulation Passwörter abfangen.

Erkennung und Sensorik

Zwar wird bei diesem Szenario davon ausgegangen, dass der Angriff über das Netzwerk erfolgt. Da allerdings die Kommunikation mit den Diensten zumindest zum Teil verschlüsselt erfolgt, stoßen Netzwerk-basierte IDS an ihre Grenzen und müssen durch weitere Sensoren ergänzt werden. Eine zuverlässigere Erkennung bieten Intrusion Detektion Systeme, die speziell die Anwendung überwachen. So existieren beispielsweise für den Apache Webserver mit ModSecurity[2] Systeme zur Überwachung des Servers. Als Ergänzung können die Log-Informationen der Anwendungen nach einem erkannten oder von außen gemeldeten Einbruch zur Analyse des Angriffs herangezogen werden.

Bewertung

Die Integrität der Server und darauf laufenden Grid-Middleware ist sehr kritisch für die Sicherheit des Grids. Die hohe Komplexität dieser Dienste läßt bislang unbekannte Schwachstellen in diesen Diensten als wahrscheinlich erscheinen. Deshalb ist die Überwachung der Grid-Middleware und die Erkennung von Angriffen durch das föderierte GIDS sehr wichtig.

A3 - Lokale Privilegieneskalation im Grid

Einordnung

Ein Angriff kann entweder über das Netzwerk oder lokal von einem am System angemeldeten Angreifer erfolgen. Hat der Angreifer die Rechte eines legitimen Benutzers, stehen diesem

[2] http://www.modsecurity.org/

weitere Angriffspunkte zur Verfügung. Beispielsweise lassen sich viele Schwachstellen im Betriebssystem nur durch Programme ausnutzen, die lokal auf dem verwundbaren System laufen.

Beschreibung

Die Worker-Nodes sind die Ressourcen des Grids, auf denen die Programme der Benutzer ausgeführt werden. Dafür wird jedem Mitglied einer virtuellen Organisation (VO) ein Benutzer-Account zugeordnet. Durch die Grid-Laufzeitumgebung wird das Programm auf die Worker-Nodes übertragen und dort mit den Rechten des jeweiligen Unix/Linux Benutzer-Accounts ausgeführt werden. Zwar begrenzen alle Betriebssysteme inklusive Windows, Unix und Linux die Rechte der Benutzer-Accounts, jedoch läßt sich dieser Schutz immer wieder durch Schwachstellen umgehen. Das größte Risiko geht dabei von Schwachstellen im Kern (Kernel) des Betriebssystems aus. Da dieser die vollständige Kontrolle über das System hat, kann ein Angreifer durch Ausnutzung einer Schwachstelle diese Rechte übernehmen. Allerdings können die Mehrzahl der Sicherheitsprobleme im Kernel nur von lokal angemeldeten Benutzern ausgenutzt werden. Da jedoch ein Benutzer berechtigt ist, Programme auf den Worker-Nodes auszuführen, entfällt diese Limitierung. Das heißt, ein Angreifer mit den Rechten eines Benutzers, kann mittels der Grid-Laufzeitumgebung, Programme zum Ausnutzen von lokalen Schwachstellen (Exploit) auf den Worker-Nodes ausführen und die vollständige Kontrolle über diese übernehmen. Dies ist insbesondere deshalb kritisch, weil ein Angreifer Programme zum Verbergen der eigenen Aktivitäten (*Root-Kits*) installieren kann.

Ein konkretes Szenario der Ausnutzung eines lokalen Root-Exploits ist in [41] beschrieben worden. Konsequenz des Angriffs ist, dass der Angreifer die vollständige Kontrolle über die Worker-Nodes erlangt. Dies ermöglicht es, das Betriebssystem beliebig zu modifizieren. Desweiteren kann, wie in [41] beschrieben, der Angreifer die erweiterten Privilegien zum Angriff auf andere Systeme im Netzwerk missbrauchen. Auf diese Weise ist unter Umständen eine Kompromittierung der Cluster-Frontends möglich. Dadurch erlangt der Angreifer Zugriff auf alle Proxy-Zertifikate, die auf dem Frontend gespeichert sind.

Erkennung und Sensorik

Da der Angriff direkt auf dem lokalen System (zum Beispiel Worker-Node) erfolgt, sind alle Netzwerk-basierten Sensoren wirkungslos. Auch lokale Sensoren sind in der Regel bei der Erkennung von lokalen Angriffen erfolglos. Allerdings lassen sich häufig die nachfolgenden Angriffe auf andere Systeme anhand der Spuren erkennen. Dies können beispielsweise Scans im Netzwerk oder erfolglose Anmeldeversuche sein. Ist der Angriff erst einmal entdeckt worden, sind die System-Logs für die Analyse des Angriffs von großer Bedeutung. Auf deren Basis läßt sich unter Umständen die ausgenutzte Schwachstelle oder Aktionen des Angreifers erkennen.

Bewertung

Aufgrund der Privilegien der Grid-Benutzer, beliebige Programme im Grid auszuführen, ist die Bedrohung durch lokale Exploits sehr hoch. Was die Bedrohung noch erhöht, ist die schlechte Erkennung dieser Angriffe durch IDS-Sensoren.

A4 - Erfolgreiche Angriffe auf Benutzer-Identitäten

Einordnung

Um Missbrauch zu vermeiden, wird die Benutzung von Grids auf eine Reihe legitimer Benutzer eingeschränkt. Für jeden Benutzer oder eine Gruppe von Benutzern (beispielsweise eine VO) werden die Rechte definiert, die diese Gruppe benötigt. Für die Sicherheit des Grids ist es deshalb wichtig, sowohl die Nutzung auf berechtigte Benutzer einzuschränken als auch deren Rechte sicher festzulegen. Für einen Angreifer ist es also ein wichtiges Ziel, unbemerkt die Identität eines Benutzers zu übernehmen, um Aktionen mit dessen Rechten ausführen zu können.

Beschreibung

Die Authentifizierung von Benutzern erfolgt über mehrere Stationen. Zuerst muss sich dieser in der Regel auf seinem lokalen Computer anmelden. Davon ausgehend authentifiziert sich der Benutzer über seinen privaten Schlüssel des X.509-Zertifikats beim Grid-Benutzerinterface. Dieses stellt ein kurzlebiges Proxy-Zertifikat aus, um Zugriff auf Grid-Ressourcen zu ermöglichen. Dadurch wird vermieden, dass der private Schlüssel des Benutzers auf Systemen im Grid gespeichert werden muss. Zwar kann auch das Proxy-Zertifikat missbraucht werden, um die Identität des Benutzer zu übernehmen, jedoch ist der Missbrauch durch die begrenzte Lebensdauer limitiert.

Die Übernahme einer Benutzer-Identität kann auf verschiedenen Wegen erfolgen. Zuerst kann die Authentifizierung vollständig umgangen werden. Beispielsweise kann ein Angreifer Wege finden, auf Ressourcen auf einem nicht autorisierten Weg zuzugreifen. Dies kann die Folge einer unsicheren Konfiguration eines Dienstes oder einer Lücke in der Authentifizierung sein. Eine weitere Möglichkeit ist das Ausnutzen von Schwachstellen im Mechanismus der Authentifizierung. Unter Umständen kann es einem Angreifer gelingen, durch eine gefälschte Identität den Zugang als Benutzer zu erlangen. Im Extremfall gelingt es dem Angreifer, die PKI zu brechen und selbst gültige Zertifikate zu erstellen. Beispielsweise ermöglicht die kürzlich gefundene Schwachstelle im TLS/SSL-Protokoll[3] in [37] einem Angreifer, Daten in eine gesicherte Verbindung einzuschleusen. Dieser Punkt wird bereits in einem folgenden Szenario in Abschnitt 4.4.5 behandelt und ist hier ausgelassen worden. Ein weiterer Angriffspunkt sind die Credentials des Benutzers selbst:

1. Der Benutzer selbst kann seine Credentials freiwillig oder unfreiwillig preisgeben.
2. Der private Computer des Benutzers kann angegriffen werden, um an das private Zertifikat zu gelangen.
3. Ein Proxy-Zertifikat kann innerhalb des Grids abgefangen werden.

Der erste Fall basiert auf der Kooperation des Benutzers. Dies kann entweder mit dem Einverständnis des Benutzers, beispielsweise durch Bestechung, oder ohne das Einverständnis durch Täuschung erfolgen. Eine häufig angewendete Methode des Social Engineerings ist das *Phishing* von Passwörtern. Dabei wird eine Massenmail mit gefälschtem Absender versendet, in der die Benutzer aufgefordert werden, in der Antwort ihre Passwörter anzugeben. Als Tendenz zeigt sich, dass auch gezielt Institutionen, wie beispielsweise Universitäten, angegriffen werden. In diesem Fall wird die Phishing-Mail an das entsprechende Institut angepaßt.

Ein wichtiger Angriffspunkt ist der private Computer des Benutzers. Läuft auf diesem ein veraltetes Betriebssystem oder sind nicht alle Sicherheits-Updates eingespielt, ist dieser ein leichtes Ziel. Der Exploit zum Ausnutzen einer Schwachstelle kann entweder per E-Mail an den Benutzer gesendet werden, oder der Benutzer wird zum Zugriff auf eine Web-Seite verleitet, die einen Exploit beinhaltet (*drive-by Exploit*). Ist der Computer kompromittiert, wird Malware nachinstalliert, die die Passwörter des Benutzers mitprotokollieren. Dies kann beispielsweise durch Manipulation des Browsers, des SSH-Client oder durch Mitprotokollieren der Tastatureingaben geschehen. Neben dem privaten Computer des Benutzers sind alle Systeme im Grid ein Angriffspunkt, auf denen Zertifikate oder Proxy-Zertifikate gespeichert werden. Allerdings kann davon ausgegangen werden, dass der Sicherheitsstandard auf diesen Systemen höher als bei privaten Computern ist. Jedoch ist der Schaden nach einer erfolgreichen Kompromittierung deutlich höher. Für eine ausführlichere Beschreibung verweisen wir auf den Abschnitt 4.4.2.

Erkennung und Sensorik

Die Übernahme einer Benutzer-Identität kann nur unter Umständen erkannt werden. Dies setzt voraus, dass Angriffe unter Verwendung von technischen Mitteln im Grid durchgeführt werden.

[3]Laut Aussage der Entwickler ist das Globus Toolkit nicht betroffen: http://lists.globus.org/pipermail/security-announce/2009-November/000012.html

Findet der Angriff außerhalb des Grids statt, ist die Kooperation des Benutzers notwendig. Dies kann beispielsweise dadurch geschehen, dass der Benutzer die Kompromittierung seines privaten Schlüssels meldet.

Bewertung

Angriffe auf die Identität eines Benutzers sind sehr wahrscheinlich. So wurde dies bereits bei Vorfällen auf Grid-Systeme beobachtet. Die Erkennung dieser Angriffe stellt sich allerdings als schwierig heraus, weil die Sensorik Angriffe nur sehr eingeschränkt erkennen kann.

A5 - Angriffe auf das Grid-IDS

Einordnung

Das Grid-IDS ist die entscheidende Komponente im Grid, die im Fall eines Angriffs diesen Erkennen soll. Die Daten des Grids liefern weiterhin wichtige Hinweise auf die Identität des Angreifers und für die Behebung des Sicherheitsvorfalls. Deshalb ist das Grid-IDS selbst ein bedeutendes Ziel für Angriffe und muss vor diesen geschützt werden.

Beschreibung

Für die Sicherheit im Grid ist es wichtig, erfolgreiche Angriffe durch das föderierte Intrusion Detection System so früh wie möglich zu erkennen. Fällt dieses System aus oder wird durch einen Angriff in der Funktion gestört, kann die Sicherheit in dem Grid nicht mehr gewährleistet werden. Aus diesem Grund ist das Grid-IDS selbst ein bedeutendes Ziel für Angriffe. Dabei muss mit den folgenden Angriffen und deren Konsequenzen gerechnet werden:

Denial of Service Diese Angriffe zielen darauf ab, die Funktion des Grid-IDS zu unterbinden oder zumindest einzuschränken. Das kann beispielsweise durch Fluten der IDS-Komponenten mit Netzwerk-Paketen oder Einbringen von gefälschten Daten (False-Positives) geschehen.

Umgehen des GIDS Fehler im Sensor zur Erkennung von Angriffen führen dazu, dass entweder erfolgreiche Angriffe übersehen (False-Negativ) oder fehlgeschlagene Angriffe fälschlich als erfolgreich (False Positive) gemeldet werden. Dabei kann ein fehlerhaftes Design des IDS oder Schwachstellen in dessen Implementierung zu diesen Fehlern führen. Insbesondere bei Netzwerk-basierten Sensoren ist es schwierig, False-postivies und False-negatives zu vermeiden. Beispielsweise kann die Komplexität des TCP-Protokolls ausgenutzt werden, um Angriffe zu verschleiern. Auf der Seite des Sensors können dadurch Limitierungen bei der Implementierung des TCP-Protokolls ausgenutzt werden, um einen Angriff unbemerkt an dem IDS vorbeizuschleusen.

Manipulation der Daten des GIDS Eine Kompromittierung von Komponenten des GIDS oder der Grid-Monitoring Umgebung, ermöglicht es einem Angreifer, Daten des GIDS zu manipulieren. Dadurch können erfolgreiche Angriffe unter Umständen nachträglich verschleiert werden oder deren Analyse wird erschwert, weil Daten fehlen oder gefälscht wurden.

Manipulation der IDS-Komponenten Im schlimmsten Fall ist ein Angreifer in der Lage, IDS-Komponenten selbst zu manipulieren oder sogar die vollständige Kontrolle über das System zu erlangen. Neben dem Missbrauch der Komponenten für Angriffe innerhalb des Grids ermöglicht dies die Verschleierung von Angriffen.

Erkennung und Sensorik

Der Aufwand der Erkennung von Angriffen auf das GIDS hängt von der Art des Angriffs und dem Vorwissen des Angreifers ab. Angriffe mit dem Ziel, das System auszuschalten sind in der Regel leicht zu erkennen. Allerdings ist hier die spezielle Schwierigkeit, den Angriff abzuwehren und das GIDS funktionsfähig zu halten. Hat der Angreifer Insiderwissen, ist davon

auszugehen, dass der Angreifer die Schwachstellen des Systems kennt und Angriffe auf das GIDS schwierig zu erkennen sind. Ähnliches gilt, wenn der Angreifer über die Privilegien eines Administrators im Grid verfügt und dadurch über effektivere Möglichkeiten zur Umgehung der Angriffserkennung verfügt.

Bewertung

Angriffe auf das Grid-IDS sind nicht unwahrscheinlich. So sind in der Praxis effektive Methoden beschrieben worden (siehe beispielsweise [46]), um Netzwerk-basierte IDS zu umgehen. Weiterhin sind in der Vergangenheit viele Programme der IT-Sicherheit inklusive von IDS und AV-Produkten von einer signifikanten Anzahl von Schwachstellen betroffen gewesen. Einige dieser Schwachstellen ermöglichten sogar die vollständige Kontrolle über diese Programme. Beispielsweise waren Snort und einige AV-Produkte von gravierenden Schwachstellen betroffen gewesen.

A6 - Denial of Service Angriffe

Einordnung

Ziel von Denial of Service Angriffen ist das Verhindern der Verfügbarkeit von Ressourcen oder zumindest deren Störung. Insbesondere bei kommerziellen Diensten ist das Risiko nicht zu vernachlässigen, dass diese einem Denial of Service Angriff ausgesetzt sind. Dabei können Angriffe entweder auf das Grid abzielen oder deren Ressourcen für Angriffe auf externe Seiten missbrauchen.

Beschreibung

Denial of Service Angriffe haben das Ziel, ein System unbrauchbar zu machen oder zumindest dessen Betrieb zu stören. Dabei muss zwischen Angriffen auf das Grid selbst und Angriffen, die vom Grid ausgehen unterschieden werden. Im ersten Fall geht es darum, den Betrieb des Grids zu stören. Dies kann beispielsweise dadurch erreicht werden, indem Komponenten des Grids angegriffen werden. Häufig geht der Angriff von einer hohen Anzahl von ferngesteuerten Systemen (beispielsweise ein Bot-Netzwerk) aus, die das Angriffsziel mit Netzwerkverbindungen oder Paketen fluten. Konsequenz ist, dass entweder das System unter der Last abstürzt oder nicht mehr erreichbar ist, weil alle Ressourcen (Bandbreite, Anzahl der Verbindungen) ausgeschöpft sind. Innerhalb des Grids bilden beispielsweise die User-Interfaces Ziele für einen Denial of Service Angriff.

Die zweite Variante sind Angriffe, die vom Grid auf externe Ziele ausgehen. Da Grids eine sehr hohe Leistungsfähigkeit im Bezug auf die Internet-Anbindung und Rechenleistung bieten, ist deren Missbrauch für diese Angriffe attraktiv. Ein Angreifer kann beispielsweise dafür einen Job auf den Worker-Nodes starten, der ein externes System mit Anfragen flutet. In wie weit dies möglich ist, hängt von den Rechten des Angreifers auf den Worker-Nodes und der Firewall-Konfiguration ab.

Erkennung und Sensorik

Es kann davon ausgegangen werden, dass Denial of Service Angriffe mit einer sehr hohe Netzwerklast einhergehen, die auf ein einzelnes System abzielt. Sie lassen sich deshalb sehr zuverlässig in den Netflows identifizieren.

Bewertung

Insbesondere bei kommerziellen Nutzungen von Grids spielt die Abwehr von Denial of Service Angriffen eine große Rolle. Die Erfahrungen zeigen, dass in der Regel diese Angriffe mit relativ geringem Aufwand entdeckt werden können. Jedoch liegt die Schwierigkeit bei deren Abwehr.

4.4.3 Kategorie Malware

In diesem Abschnitt werden die Szenarien der Kategorie „Einsatz Malware auf Grid-Systemen“ beschrieben. Diese sind analog zu den vorherigen Szenarien mit M1 bis Mn durchnummeriert.

M1 - Einsatz von Root-Kits

Einordnung

Root-Kits werden typischerweise in Verbindung mit anderer Malware eingesetzt, um diese aus Sicht des Betriebssystems zu verbergen. Inzwischen sind technisch aufwendige Root-Kits für alle Betriebssysteme veröffentlicht worden.

Beschreibung

Ein Root-Kit dient zum Verbergen der Aktionen eines Angreifers nach einer erfolgreichen Kompromittierung des Systems. Dafür wird das System in einer Art und Weise manipuliert, dass ausgewählte Dateien, Prozesse, Netzwerk-Sockets und unter Windows Registry-Keys nicht mehr durch die Standard-Funktionen des Betriebssystems angezeigt werden.

Dafür gibt es mehrere Alternativen. Die ersten Root-Kits unter Unix haben typischerweise die System-Kommandos *ls*, *ps*, *netstat* manipuliert. Dies läßt sich allerdings leicht erkennen, indem die Integrität der entsprechenden Binaries kontrolliert geprüft wird. Spätere Root-Kits haben deshalb den Kern des Betriebssystems manipuliert, weil dessen Manipulation nur mit deutlich größerem Aufwand zu erkennen ist. Inzwischen verwenden die aktuellen Root-Kits immer ausgefeiltere Methoden, um die Erkennung zu erschweren. Eine davon ist, das Betriebssystem im laufenden Betrieb in eine virtuelle Maschine zu verschieben. Das Root-Kit läuft dann innerhalb des Monitors der virtuelle Maschine. Zwar setzt diese Vorgehensweise die Unterstützung durch aktuelle Prozessoren voraus. Jedoch lassen sich diese Root-Kits im laufenden Betrieb nur extrem schwer erkennen. Der Grund dafür ist, dass der Prozessor dem virtuellen Betriebssystem keine Möglichkeit bietet, herauszufinden, ob es virtualisiert wurde. Ein Beispiel ist das Root-Kit *Blue Pill*, dessen Quellcode bereits veröffentlicht wurde.

Erkennung und Sensorik

Weil sich Root-Kits aktiv schützen, sind sie nur sehr schwer und mit aufwendigen Methoden zu finden. Zudem ist eine Erkennung über das Netzwerk nicht möglich. Für bekannte Root-Kits gibt es eine Reihe von spezialisierten Programmen. Beispiel ist Microsofts RootkitRevealer. Allerdings stellen auch die meisten bekannten Hersteller von AV-Produkten Erkennungsprogramme zur Verfügung. Diese suchen entweder direkt nach Spuren des Root-Kits im Speicher oder Dateisystem. Alternativ wird nach Spuren des typischen Verhaltens von Root-Kits gesucht. Ansatzpunkt der Erkennung bieten die Manipulationen, die am Betriebssystem durchgeführt werden. Dafür reimplementiert das Erkennungsprogramm die Funktionen des Betriebssystems zum Zugriff auf das Dateisystem und die Prozess-Liste. Dann wird eine Liste der Dateien oder Prozesse jeweils mit den originalen Funktionen und den reimplementierten erstellt. Im Fall eines integeren Betriebssystem stimmen beide Listen überein. Werden jedoch Dateien oder Prozesse verborgen, fällt dies bei dem Vergleich auf.

Bewertung

In bekannten Vorfällen in Grid-Systeme wurde das Phalanx2 Root-Kit eingesetzt (siehe [49]). Die Gefahr des Einsatz ist also in der Praxis sehr hoch und es ist wichtig, diese Bedrohung zu berücksichtigen.

M2 - Einsatz von trojanisierter oder manipulierter Software

Einordnung

Die Manipulation oder Trojanisierung von Programmen ist bei Sicherheitsvorfällen üblich. Dabei ist es wichtig, diese Manipulationen zu erkennen, um kompromittierte Systeme zu erkennen

und diese in einen integeren Zustand zu überführen.

Beschreibung

Software wird mit unterschiedlichen Zielsetzungen manipuliert:

- **Ausspionieren des Benutzers**: Häufig werden der Internet-Browser oder SSH-Client oder Server manipuliert, um an die Passwörter des Benutzers zu gelangen (*Spyware*). Darauf wurde bereits in dem Szenario A4 eingegangen. Kritischer ist die Manipulation zentraler Komponenen wie beispielsweise SSH-Server, um Passwörter aufzuzeichnen.

- **Unautorisierter Zugang**: Nach einem erfolgreichen Einbruch werden Hintertüren angelegt, damit sich der Angreifer unter Umgehung der vorhandenen Mechanismen zur Authentifizierung am System anmelden kann. Beispiel sind manipulierte Web- oder SSH-Server. Deren Entdeckung auf dem lokalen System wird häufig durch Root-Kits verhindert (siehe Szenario M1).

- **Verbergen von Informationen**: Root-Kits (Szenario M1) manipulieren Systemkommandos oder den Kern des Betriebssystem, um Informationen zu verbergen. Damit verhindert das Root-Kit seine eigene Entdeckung und die von Hintertüren und weiterer Malware.

- **Angriff auf andere Systeme**: Typisches Beispiel ist die Manipulation von Web-Servern. Diese werden so manipuliert, dass Exploits zum Angriff auf Internet-Browser in alle ausgelieferten Web-Seiten eingefügt wird, beispielsweise als *iframe*. Verbindet sich ein Benutzer zu dem Web-Server und ruft dort eine Seite auf, wird der Browser der Benutzers automatisch angegriffen (*Drive-by-Exploit*).

Insbesondere kritisch ist die Erkennung der Manipulationen, wenn die Grid-Middleware davon betroffen ist. Darauf wird im folgenden Abschnitt 4.4.4 eingegangen. Allerdings ist auch die Erkennung von Hintertüren und Root-Kits bei der Wiederherstellung von Systemen nach einem Einbruch sehr wichtig.

Erkennung und Sensorik

Die Erkennung hängt vom Einsatzzweck ab. Hintertüren und Spyware lassen sich prinzipiell an deren Netzwerkverkehr erkennen, wenn sich dieser vom legitimen unterscheidet. Unterschiede zu legitimen Netzwerkverkehr können durch die Verwendung ungewöhnlicher Ports oder Verbindungen zu unbekannten IP-Adressen erkannt werden. Ein Beispiel sind Verbindungen vom SSH-Server zu unbekannten IP-Adressen.

Weiterhin lassen sich Manipulationen an Programmen durch Überprüfen der Integrität der Hash-Werte erkennen. Leider stößt diese Methode beim Kernel auf Grenzen, weil dessen Komponenten (zum Beispiel Module und Datenstrukturen) nicht statisch sind.

Bewertung

Die Erfahrung zeigt, dass die Manipulation von Programmen im Grid eine realistische Bedrohung ist. So wird in [50] von Vorfällen im Grid berichtet, bei denen der SSH-Server zum Aufzeichnen der Passwörter manipuliert wurde.

M3 - Aufbau von Bot-Netzwerken

Einordnung

Wie bereits in dem Threat Report von Symantec in [45] beschrieben wurde, sind Netzwerke aus kompromittierten Systemen (Bot-Netzwerke) eine ernste Bedrohung. Die größte Gefahr geht dabei von der Größe der Netzwerke aus, die sich von einer zentralen Stelle aus steuern lassen.

Beschreibung

Als Bot-Netzwerk wird eine Gruppe von Systemen bezeichnet, die von einer zentralen Stelle aus gesteuert werden. Dabei werden Bot-Netzwerke fast immer auf der Basis kompromittierter Systeme aufgebaut. Typischerweise werden Bot-Netzwerke zum Versenden von Spam E-Mails, Durchführung automatisierter Angriffe und verteilte Denial of Service Angriffe verwendet.

Aus der Sicht eines Angreifers haben Bot-Netzwerke folgende Vorteile:

- Sie sind hochgradig redundant und können flexibel skaliert werden, das heißt, wenn Systeme in dem Netzwerk ausfallen, können andere Systeme die Funktionalität übernehmen.
- Weitere Systeme lassen sich ohne Aufwand in das Bot-Netzwerk integrieren.
- Die Bot-Netzwerke lassen sich von einer zentralen Stelle aus kontrollieren.
- Ein Angreifer kann so dem Bot-Netzwerk Kommandos zum simultanen Angriff auf ein einzelnes System (DDoS Angriff) oder zur parallelen Ausführung eines Kommandos auf allen Systemen verteilen.

Damit weisen Bot-Netzwerke viele Ähnlichkeiten zu Grids auf.

Für den Aufbau eines Bot-Netzwerkes werden viele Systeme ungezielt angegriffen. Das kann auf verschiedenen Arten erfolgen:

- Versenden von E-Mails mit dem Bot als Anhang oder Exploit zum Ausnutzen einer Schwachstelle.
- Manipulation eines Web-Servers zum Angriff auf Browser. Wie in Abschnitt 4.4.3 beschrieben wird ein Web-Server zum Angriff auf Internet-Browser manipuliert.
- Das Bot-Netzwerk selbst wird zum Angriff ausgenutzt. Dazu kann der Angreifer ein Kommando an das Bot-Netzwerk senden, durch dessen Folge ein bestimmtes Netzwerk automatisiert angegriffen wird.
- Ein Internet-Wurm wird zum Angriff auf möglichst viele Systeme frei gesetzt.

Auf den erfolgreich kompromittierten Systemen wird ein Bot installiert, über den das System kontrolliert wird. Die Kommunikation zwischen Bot und Angreifer kann in zwei Alternativen erfolgen:

Zentraler Server Jeder Bot ist mit einem zentralen Server verbunden. Für die Kommunikation werden typischerweise die Protokolle HTTP und IRC verwendet. In diesem Fall erhalten die Bots die Kommandos von dem Server über IRC oder HTTP. Im Fall von IRC verbinden sich alle Bots zu einem vom Angreifer vorgegebenen Server und treten einem IRC-Channel bei. Der Angreifer kann die Bots kontrollieren, indem dieser Kommandos in den IRC-Channel eingibt, die dann an die Bots verteilt werden. Alternativ rufen die Bots periodisch über HTTP eine Web-Seite des Angreifers auf, die die entsprechenden Kommandos an die Bots beinhaltet.

Peer-to-Peer Jeder Bot hat eine Liste mit Peers, über die dieser Nachrichten austauscht. Vorteil dieser Variante aus der Sicht des Angreifers ist das Fehlen eines zentralen Ausfallpunktes. Nachteil ist die deutlich aufwendigere Synchronisation des Bot-Netzwerkes.

Erkennung und Sensorik

Bot-Netzwerke mit zentraler Steuerung lassen sich am effektivsten durch die charakteristische Kommunikation finden. Ist erst einmal ein Bot identifiziert, resultiert dessen Analyse in der Adresse des Kontroll-Servers. Durch Rückverfolgung der Systeme, bei denen analog eine Verbindung zu dem Kontroll-Server bestand, lassen sich die restlichen Bots des Netzwerkes finden.

Diese Methode funktioniert bei Peer-to-Peer Netzwerken nur eingeschränkt. Hier lassen sich nur die nächsten Peers herausfinden. Können allerdings charakteristische Merkmale in der Kommunikation gefunden werden, lassen sich weitere Bots durch Auswertung der Netflows bestimmen.

Bewertung

Bot-Netzwerke sind für das Internet eine ernste Bedrohung und spielen insbesondere beim kommerziellen Missbrauch von Computersystemen eine bedeutende Rolle. Es muss davon ausgegangen werden, dass Grids ein lohnenswertes Ziel für alle Betreiber von Bot-Netzwerken darstellen.

Eine Alternative ist, dass einzelne oder mehrere Systeme im Grid (beispielsweise Worker-Nodes) in ein bestehendes Netzwerk integriert werden. Aufgrund der Ähnlichkeiten zwischen Bot-Netzwerken und Grids ist allerdings auch möglich, dass die Grid-Infrastruktur selbst als Bot-Netzwerk missbraucht wird.

4.4.4 Kategorie Ressourcen

In diesem Abschnitt werden die Szenarien der Kategorie „Missbrauch und Verletzung von Ressourcen“ beschrieben. Diese sind analog zu den vorherigen Szenarien mit R1 bis Rn durchnummeriert.

R1 - Missbräuchliche Nutzung von Compute- und Storage-Ressourcen

Einordnung

In diesem Abschnitt wird der Missbrauch von Gridressourcen beschrieben. Zunächst wird darauf eingegangen, dass die große Rechenleistung von Gridumgebungen für illegale Zwecke genutzt werden kann. Im zweiten Teil wird beschrieben, wieso Storage-Ressourcen ebenfalls ein potentielles Ziel für Angriffe darstellen können und welche rechtlichen Auswirkungen dies hat.

Beschreibung

Grid-Infrastrukturen dienen der Berechnung komplexer Probleme in hinnehmbarer Zeit. Für diese Berechnungen werden häufig sehr große Datenmengen benötigt. Diese können beispielsweise als Eingabe für Berechnung erforderlich sein. Ebenso können große Datenmengen das Ergebnis einer Berechnung sein. In Gridumgebungen werden verschiedene Arten von Ressourcen eingesetzt, um die gegebenen Anforderungen zu erfüllen. Man unterscheidet in erster Linie zwischen sogenannten Compute-Ressourcen und Storage-Ressourcen.

Um die große Rechenleistung eines Grids / Clusters für illegale Zwecke auszunutzen, muss nicht zwangsläufig ein Angriff vorausgehen. Auch ein autorisierter Gridbenutzer ist in der Lage, solche Gridjobs auszuführen. So könnte ein Benutzer beispielsweise die zur Verfügung stehende Rechenleistung dazu nutzen, mit geeigneten Programmen / Algorithmen ein Passwort mittels eines Brute-Force-Angriffs zu erlangen. Ein solcher Angriff wird erheblich weniger Zeit benötigen, als auf einem Heimcomputer. Das gelingt natürlich nur unter der Voraussetzung, dass dem Angreifer ein gut parallelisierter Algorithmus zur Verfügung steht und sich so die Anzahl der zu testenden Kennworte pro Sekunde steigern ließe. Auch für andere Arten des Missbrauchs, wie beispielsweise dem Aushebeln von Kopierschutzmechanismen urheberrechtlich geschützter Medien könnten die Compute-Ressourcen verwendet werden.

Aber auch die in einer Grid-Infrastruktur bereitgestellten, großen Datenspeicher könnten durch einen Angreifer für seine Zwecke missbraucht werden. Ein Gridbenutzer ist technisch in der Lage, beliebige Daten auf den Storage- Ressourcen zu speichern. Neben der Speicherung der Daten besteht ebenso die Gefahr, dass es dem Angreifer gelingt, die auf den Storage-Ressourcen liegenden Daten an Dritte weiter zu verteilen. Aber nicht erst das Verteilen, sondern auch schon

das bloße Speichern von Daten kann zu juristischen Problemen führen, wenn es sich hierbei zum Beispiel um urheberrechtlich geschützte oder illegale Inhalte handelt.

Im D-Grid bedient man sich einer Acceptable Use Policy (AUP) um sich juristisch gegen den Missbrauch von Gridressourcen abzusichern. Diese Einverständniserklärung muss von allen Benutzern im D-Grid unterzeichnet werden, bevor sie Zugriff auf die Ressourcen erhalten. Jeder einzelne Benutzer akzeptiert somit, dass keine illegalen oder urheberrechtlich geschützten Inhalte über das D-Grid verbreitet werden dürfen. Ebenso ist das Einbringen und Verbreiten von Viren, sowie anderen Schadprogrammen verboten. Auch dürfen sich die Benutzer keine personenbezogenen Daten aus den Diensten und Ressourcen des D-Grids verschaffen. Durch die AUP können sich die Ressourcenbetreiber rechtlich absichern. Die Entdeckung und Verhinderung solcher illegaler Nutzungen des Grids sind dagegen ein technisches zu lösendes Problem.

Erkennung und Sensorik

Der Missbrauch der Ressourcen des Grids kann alleine vom Zweck und dem Ursprung der Daten (beispielsweise urheberrechtlich geschützte Inhalte) abhängen. In diesem Fall liegt kein Angriff als solcher vor und eine automatische Erkennung des Missbrauchs ist deshalb nicht möglich. Das ist nur dann möglich, wenn Ressourcen durch den Missbrauch (beispielswesise Rechenleistung oder Speicherkapazität) erschöpft sind oder deren Gebrauch von der legitimen Verwendung abweichen.

Bewertung

Der Missbrauch von Ressourcen ist in vielen Fällen weniger ein technisches, sondern mehr ein juristisches Problem. In diesen Fällen liegt kein direktes Sicherheitsproblem vor und eine organisatorische Absicherung in Form einer Acceptable Use Policy ist ausreichend.

R2 - Ausspähen vertraulicher Daten auf Gridressourcen

Einordnung

In diesem Abschnitt wird aufgezeigt, welche Arten von vertraulichen Daten sich in einem Grid befinden können und mit welchen Angriffen diese ausgespäht werden könnten. Hierfür ist teilweise kein Angriff von außen notwendig. Auch durch autorisierte Gridbenutzer könnten entsprechende Daten erlangt werden.

Beschreibung

Im D-Grid gibt es eine Vielzahl von Gridbenutzern verschiedenster Fachgebiete. Unter anderem handelt es sich hierbei um Benutzer, die medizinische Berechnungen im Grid durchführen [32]. Die hierfür im Grid verwendeten medizinischen Daten erfordern hohe Sicherheitsstandards bezüglich Vertraulichkeit und Integrität der Daten. Dies gilt jedoch nicht nur für solch medizinische Anwendungen, sondern vielmehr für alle personenbezogenen Daten, die dem Datenschutz unterliegen.

In Zukunft sollen im D-Grid auch kommerzielle Projekte durchgeführt werden. Kunden aus der Wirtschaft legen sehr großen Wert auf die vertrauliche Behandlung ihrer Daten. Komplexe Berechnungen, die in einem Grid realisiert werden könnten, werden in vielen Wirtschaftsbereichen benötigt. Als Beispiel sei die Automobilindustrie genannt, die durch aufwendige Crash-Simulationen die Kosten bei der Entwicklung neuer Sicherheitskonzepte massiv reduzieren kann. Durch Spionage oder das Ausspähen von Berechnungsergebnissen kann einem solchen Unternehmen ein großer finanzieller Schaden entstehen. Ein Wettbewerbsnachteil kann aber zum Teil schon entstehen, indem bekannt wird, dass ein Unternehmen große Berechnungen im Grid durchgeführt hat. Auch diese Informationen müssen deshalb streng vertraulich behandelt werden. Die Manipulation von Daten ist eine weitere wesentliche Bedrohung. Hierzu zählt neben der Verfälschung von Ergebnissen und der dadurch entstehenden Zerstörung von Forschungsbemühungen auch die Löschung von berechneten Daten.

Einem Angreifer (möglicherweise ein normaler, authentifizierter und autorisierter Gridbenutzer), der auf die Daten anderer Zugriff erlangen möchte, stehen mehrere potentielle Angriffspunkte zur Auswahl. Ein möglicher Ansatz wäre die Ausnutzung von fehlerhaft konfigurierten ACLs oder andere lokale Sicherheitslücken, die es erlauben auf Daten anderer Benutzer lesend oder gar schreibend zuzugreifen.

Ein im Gridumfeld weiterer wichtiger Ansatz ist der Diebstahl von Credentials. Im D-Grid erfolgt die Authentifizierung mittels X.509-Zertifikaten. Jeder Gridbenutzer erhält zunächst ein solches Zertifikat und führt damit Gridjobs aus. Durch das Zertifikat wird die Identität eines Benutzers an seinen (im Rahmen einer PKI [18] vergebenen) öffentlichen Schlüssel gebunden. Daten, die sich im Laufe eines Gridjobs in der Gridumgebung befinden, können anhand des Zertifikats und des entsprechenden privaten Schlüssels bezüglich der Integrität und der Vertraulichkeit abgesichert werden. Um im Grid Computing erforderliche Delegationen und das sogenannte Single Sign-on realisieren zu können, werden Proxy Credentials [23] verwendet. Ein Credential besteht aus einem Proxy-Zertifikat und dem dazu passenden privaten Schlüssel. Diese Proxy Credentials liegen aus technischen und konzeptionellen Gründen in heutigen Gridumgebungen unverschlüsselt auf verschiedenen Gridressourcen vor. Ein Angreifer, der Zugriff auf diese Credentials erlangen kann, hat im Folgenden die Möglichkeit, im Namen des Besitzers im Grid zu agieren. Ein Zugriff auf diese Daten im lokalen Dateisystem der Ressourcen ist dementsprechend besonders sicherheitskritisch.

Einige Gridmiddlewares bieten sogenannte Community- bzw. Pool-Accounts. Um nicht für jeden Benutzer des Grids einen eigenen lokalen Account verwalten zu müssen, werden Benutzer dynamisch auf die vorhandenen Accounts abgebildet. Die Gefahr hierbei besteht darin, dass nach der Beendigung eines Gridjobs alle Daten des Gridjobs aus dem Account entfernt werden müssen. Sollten hingegen Daten im Account verbleiben, so besteht für den nächsten Benutzer, der auf diesen Account abgebildet wird, die Möglichkeit, die noch vorhandenen Daten zu lesen.

Ein weiterer Ansatzpunkt für einen Angriff sind Accounting- und Billingdaten. Ein Angreifer, der auf einer Gridressource die nötigen Rechte erlangt hat, könnte dafür sorgen, dass alle oder nur die für ihn entscheidenden Accounting- und Billingdaten umgeleitet beziehungsweise ebenfalls an ihn gesendet werden. Auch diese müssen vertraulich behandelt werden und dürfen keinesfalls in die Hände Dritter gelangen.

Erkennung und Sensorik

Zuerst kann durch eine Angriff eine Schwachstelle ausgenutzt werden, um an die Daten zu gelangen. In diesem Fall greift die Sensorik zur Erkennung von Angriffen, wie es in den Angriffsszenarien beschrieben wurde. Allerdings kann der nicht-autorisierte Zugriff auf vertrauliche Daten auch durch eine Fehlkonfiguration ausgelöst werden. In diesem Fall läßt sich der Zugriff nicht direkt durch einen Sensor erkennen. Jedoch kann dieser eventuell noch in den System-Logs nachvollzogen werden.

Bewertung

Es ist zu berücksichtigen, dass die Erkennung des Angriffs nicht vor deren Diebstahl schützt. Vertrauliche Daten der Anwender oder der Grid-Verwaltung lassen sich aus diesem Grund am effizientesten mit den bekannten Methoden der Kryptographie schützen.

R3 - Manipulation von Grid-Ressourcen

Einordnung

In diesem Abschnitt wird beschrieben, wie die Gridressourcen verändert werden können, um unberechtigten Dritten Zugriff zu gewähren beziehungsweise bestehenden Benutzern den Zugriff zu verweigern. Ebenso wird erläutert, auf welche Weise ein Angreifer unbemerkt im Grid Jobs berechnen lassen könnte.

Beschreibung

Wie bereits in Szenario R2 beschrieben, kann ein Angreifer dafür sorgen, dass die auf einer Gridressource anfallenden Accounting- und Billing-Daten zum Angreifer umgeleitet werden können. Auf diese Weise könnten vertrauliche Daten über die laufenden Gridjobs verbreitet werden. Neben dem Ausspähen dieser Daten ist die Fälschung ein mindestens genauso großes Sicherheitsrisiko. Ein Angreifer könnte dafür sorgen, dass anfallende Accounting- und Billing-Daten nicht direkt an den korrekten Service gesendet werden, sondern zuvor durch ein entsprechendes Skript oder Programm manipuliert werden. So könnte ein Angreifer auf Gridressourcen Jobs rechnen lassen und durch die Manipulation der Accounting- und Billing-Daten dafür sorgen, dass die hierfür benötigte Rechenzeit einem anderen Benutzer in Rechnung gestellt wird.

Eine weitere, ernst zunehmende Gefahr besteht in Änderungen beziehungsweise dem Austausch von Sicherheitsbibliotheken und Programmen, die auf diese Bibliotheken zurückgreifen. Im Gridumfeld wird für grundlegende Funktionen zur Sicherheit die Grid Security Infrastructure (GSI) genutzt. Hat ein Angreifer die volle Kontrolle über das Dateisystem auf einer Gridressource, so ist er auch in der Lage, die entsprechenden GSI-Bibliotheken zu verändern beziehungsweise bereits manipulierte Komponenten einzuspielen. Durch diese Veränderungen können Sicherheitsabfragen umgangen und vorgetäuscht werden. Ebenso wäre auf diese Weise die Nutzung nicht vertrauenswürdiger Zertifikate möglich. Vielfältige andere Möglichkeiten des Missbrauchs sind hierbei denkbar. Daher ist die Manipulation von Sicherheitsbibliotheken stets zu verhindern und zu überwachen. Diese Bedrohung ist auch Teil des Szenarios M2.

Im D-Grid gibt es zur Zeit 32 Virtuelle Organisationen (VOs). Alle Gridbenutzer sind einer oder mehreren VOs zugeordnet. Im Gegenzug werden Berechtigungen auf den einzelnen Gridressourcen VO-weit vergeben. Aus der Kombination dieser beiden Informationen werden auf den einzelnen Gridressourcen die sogenannten grid-mapfiles erzeugt. In dieser Datei werden Gridbenutzer auf lokale Benutzerkonten abgebildet. Dies geschieht nicht zuletzt deswegen, weil man bei aufgetretenen (Sicherheits-)Vorfällen nachvollziehen können möchte, welcher Gridbenutzer lokal auf einer Gridressource gerechnet hat. Ein Angreifer könnte versuchen, das vorhandene Mapping dahingehend zu manipulieren, seine eigenen Aktionen im Grid zu verschleiern.

Ein ebenfalls ernst zunehmendes Szenario ist die Erlangung der Kontrolle über die Grid Ressource Registry Service-Datenbank (GRRS-DB) bzw. Virtual Organization Membership Service-Datenbank (VOMS-DB). Einerseits könnte ein Angreifer so neue Ressourcen hinzufügen oder die VO-Berechtigungen auf Gridressourcen verändern. Andererseits wäre es auch möglich, dass ein Angreifer in der VOMS-DB beliebige neue Benutzer anlegt oder bestehende Benutzerdaten verändert oder löscht. Der direkte Zugriff auf eine dieser Datenbanken ist zwar unwahrscheinlich, bietet aber bei Gelingen ein großes Potential an möglichem Schaden.

Erkennung und Sensorik

Wie in dem Szenario R2 in Abschnitt 4.4.4 sind in der Regel vorangehende Angriffe für die Manipulation notwendig. Dafür wird auf die Angriffs-Szenarien verwiesen. Zusätzlich läßt sich die Manipulation von Ressourcen durch kryptografische Methoden erkennen. Dies ist allerdings schwierig, wenn die Daten dynamisch geändert werden.

Bewertung

Da die für den operativen Betrieb des Grids notwendigen Daten sicherheitskritisch sind, ist ein Schutz vor deren nicht-autorisierter Manipulation notwendig. Zwar kann die Integrität durch kryptographische Methoden angesichert werden, jedoch ist diese schwierig für Daten, die sich dynamisch ändern (beispielsweise Inhalte von Datenbanken). In diesem Fall ist also die Erkennung des vorhergehenden Angriffs wichtig.

4.4.5 Kategorie Schwachstellen

In diesem Abschnitt werden die Szenarien der Kategorie „Ausnutzung von Schwachstellen“ beschrieben. Diese sind analog zu den vorherigen Szenarien mit S1 bis Sn durchnummeriert.

S1 - Schwachstellen in der Grid PKI

Einordnung

In diesem Abschnitt geht es weniger um ein Grid-spezifisches Angriffsszenario, als vielmehr um eine dem Grid zugrunde liegende Technik zur Sicherung von Ressourcen und Kommunikation im Grid. Die Public Key Infrastructure (PKI) wird in diesem Abschnitt kurz beschrieben und es wird erläutert an welchen Stellen ein Angriffsversuch möglich wäre und wie sinnvoll und erfolgversprechend dieses Vorhaben wäre.

Beschreibung

Im D-Grid kommt eine Public Key Infrastructure (PKI) für die Sicherung von Ressourcen und der Kommunikation innerhalb des Grids zum Einsatz. Die Grundlage der PKI ist die Ver- und Entschlüsselung von Nachrichten mithilfe von öffentlichen und privaten Schlüsseln. Neben der Vertraulichkeit von Nachrichten kann ebenso die Integrität einer Nachricht mithilfe der PKI sichergestellt werden. Nachrichten, die mithilfe eines privaten Schlüssels signiert werden, können auf dem Weg zu Ihrem Empfänger nicht durch einen unbefugten Dritten geändert werden, ohne dass dies vom Empfänger erkannt werden kann (Integrität). Verschlüsselt der Sender eine Nachricht mit dem öffentlichen Schlüssel des Empfängers, so ist niemand anderes als der Empfänger in der Lage, die Nachricht zu entschlüsseln.

Im Gridumfeld wird mit sogenannten X.509-Zertifikaten [21] gearbeitet. Diese Zertifikate enthalten den oben genannten öffentlichen Schlüssel eines Benutzers beziehungsweise einer Ressource. Ausgegeben werden die Zertifikate von einer Certificate Authority (CA). Eine auf diese Weise aufgebaute PKI kann nur dann funktionieren und den erforderten Schutz bieten, wenn die folgenden drei wesentlichen Voraussetzungen erfüllt sind:

Vertrauen in die CA: Alle zur PKI gehörigen Benutzer und Ressourcen müssen Vertrauen in die übergeordnete CA haben.

Schutz vor Kompromittierung: Keinesfalls darf der zur einem Zertifikat beziehungsweise dem enthaltenen öffentlichen Schlüssel passende private Schlüssel in die Hände eines unbefugten Dritten geraten. Der Besitzer des privaten Schlüssels kann in Zusammenhang mit dem Zertifikat im Namen des ursprünglichen Benutzers agieren. Eine besondere Gefahr stellt die Kompromittierung von privaten Schlüsseln von CAs dar. Gelangt ein solcher privater Schlüssel in die Hände eines Dritten, so ist nicht nur die CA selbst von diesem Vorfall betroffen, sondern alle von ihre herausgegebenen Zertifikate. Wird also das Zertifikat einer CA ungültig, so werden mit ihm alle von ihr ausgestellten Zertifikate mit ungültig. Gerade bei großen CAs wäre dies ein immenser wirtschaftlicher Schaden.

Zurückziehen kompromittierter Zertifikate: Sollte die Kompromittierung eines Benutzer- beziehungsweise Hostzertifikats erkannt worden sein, so muss die Möglichkeit bestehen, die Gültigkeit dieses Zertifikats so schnell wie möglich zu widerrufen. Dies geschieht auf technisch über sogenannte Certificare Revocation Lists (CRL) oder auch das sogenannte Online Certificate Status Protocol (OCSP) [22].

Im Wesentlichen gibt es drei Arten, wie man eine solche PKI angreifen könnte. Zum einen kann die übergestellte CA angegriffen werden, zum anderen sind aber auch Angriffe auf die intern verwendeten Verschlüsselungsalgorithmen denkbar. Eine dritte Möglichkeit wäre der Versuch, die PKI zu umgehen.

Wie bereits erwähnt, ist die sichere Verwahrung des privaten Schlüssels einer CA Grundvoraussetzung für den Aufbau einer PKI. Sollte ein unbefugter Dritter Zugang zum privaten

Schlüssel einer CA erhalten, so wäre er in der Lage, beliebige Benutzeridentitäten zu bestätigen und auf diese Weise das Vertrauen in die PKI zu zerstören. Auch die Fälschung und gefälschte Signatur von CRLs wäre denkbar. Im D-Grid gibt es zwei ausstellende CAs: die GridKa-CA des Forschungszentrums Karlsruhe und die DFN-Grid-CA des DFN-Vereins. Diese beiden CAs sind EuGridPMA-zertifiziert [11] und entsprechen daher dem erforderlichen Standard. Eine weitere Möglichkeit, die PKI empfindlich zu stören, wäre es, CRL-Repositories oder OCSP-Server einer Denial-of-Service Attacke (DOS) auszusetzen. Auf diese Weise könnte verhindert werden, dass bereits zurückgezogene Zertifikate korrekt erkannt und bei einer Validierung als ungültig markiert werden würden.

Eine andere, wesentlich ernster erscheinende Gefahr ist der Angriff auf intern verwendete Verschlüsselungsalgorithmen. Es ist festzustellen, dass nur äußerst selten Sicherheitslücken in etablierten und gebräuchlichen Verschlüsselungsalgorithmen gefunden und ausgenutzt werden. Ein solches Beispiel stellt der von Stevens im letzten Jahr vorgestellte Angriff auf den MD5-Hash [44] dar.

Meistens handelt es sich hingegen lediglich um Sicherheitslücken in den Implementierungen der bekannten Algorithmen, die durch einen Bugfix meist innerhalb kürzester Zeit geschlossen werden können. Allerdings kann auch das Protokoll selbst von einer Sicherheitslücke betroffen sein, was deren Behebung deutlich erschwert. Beispiel ist die Schwachstelle im SSLv3 und TLS Protokoll. Diese besteht aufgrund eines Fehlers beim Design der TLS-Renegotiation (siehe [37]). Die Schwachstelle ermöglicht einem Angreifer, Daten in eine TLS-Verbindung einzuschleusen. Insbesondere beim HTTPS Protokoll sind Szenarien gefunden worden, unter denen die Schwachstelle ausgenutzt werden kann.

Erkennung und Sensorik

Schwachstellen in der Grid-PKI lassen sich nur im Fall von direkten Angriffen auf technische Systeme erkennen. Dies kann beispielsweise ein Denial of Service Angriff gegen eine Sperrliste sein. Das Ausnutzen von Schwachstellen im Protokoll und in den Algorithmen läßt sich grundsätzlich nicht durch technische Sensoren erkennen. In diesem Fall sind wieder organisatorische Maßnahmen wie die Zusammenarbeit mit einem CERT wichtig.

Bewertung

Zwar kann der Schaden durch Schwachstellen in der PKI die Sicherheit des Grid vollständig unterwandern. Jedoch zeigt die geringe Anzahl der in der Vergangenheit gefunden gravierenden Schwachstellen, dass diese Bedrohung relativ gering ist. Zudem lassen sich diese Schwachstellen häufig nur mit hohem Aufwand ausnutzen.

S2 - Ausnutzung von unbekannten Schwachstellen

Einordnung

Die Mehrzahl der Angriffen gilt bekannten Schwachstellen. Allerdings muss auch mit Angriffen auf noch nicht veröffentlichte Schwachstellen gerechnet werden.

Beschreibung

Die meisten Schwachstellen in Softwareprodukten werden entweder vom Hersteller, von IT-Sicherheitsunternehmen oder unabhängigen Forschern gefunden. Im Rahmen der verantwortungsvollen Veröffentlichung werden die Schwachstellen zuerst dem Hersteller gemeldet und erst dann veröffentlicht, nachdem ein Update zum Schließen verfügbar ist. Allerdings wird im IT-Untergrund auch aktiv nach neuen Schwachstellen gesucht, die für kriminelle Zwecke missbraucht werden können. Ein Programm zum Ausnutzen dieser nicht öffentlich bekannten Schwachstellen wird als *zero-day Exploit* bezeichnet. Aus der Sicht der Angreifer ist der große Vorteil, dass kein wirksamer Schutz vor Angriffen verfügbar ist. Wie im Symantec Threat Report beschrieben wird, ist die Wahrscheinlichkeit eines zero-day Exploits bei Internet-Browsern, Office Anwendungen und Web-Anwendungen relativ hoch.

Erkennung und Sensorik

Ist eine Schwachstelle bekannt, kann in der Regel eine charakteristische Signatur für Angriffe auf diese Schwachstelle erstellt werden. In diesem Fall lassen sich die Angriffe effizient durch ein netzwerk-basiertes IDS erkennen. In dem Fall eines zero-day Exploits fehlt eine derartige Signatur. Das erschwert die Erkennung von Angriffen erheblich. Einzige Chance existiert durch Honeypots oder lokalen IDS mit generischer Angriffserkennung. Beispielsweise ist im Rahmen des NoAH Projektes der *Argos* Honeypot getestet worden, der diese Eigenschaften erfüllt.

Bewertung

Von zero-day Exploits sind typischerweise Web-Anwendungen und Internet-Browser betroffen. Wie bereits oben beschrieben, sind davon auch die Web-Anwendungen in Grids und privaten Computer der Benutzer betroffen. Aus diesem Grund sind zero-day Exploits eine ernsthafte Bedrohung für Grids.

4.5 Bewertung der Szenarien

Ziel der Bedrohungsanalyse ist ein Anforderungskatalog an das Grid-IDS. Die Grundlage dafür bildet die Bewertung der Szenarien. Dabei werden die Anforderungen prioristiert, die sich aus den für das Grid-IDS wichtigsten Szenarien ableiten.

In diesem Abschnitt werden die Szenarien in tabellarischer Form aufgelistet und bewertet. Für jedes Szenario werden dabei die Wahrscheinlichkeit, der Aufwand der Abwehr, der Schaden und das daraus resultierende Risiko benotet. Da für Grids keinerlei Statistiken über Angriffe vorliegen und sich im Allgemeinen der Schaden nur sehr schwer bemessen läßt, wird bewusst auf eine quantitative Risikoabschätzung verzichtet. Grundlage ist ein Abschätzung dieser Werte auf der Basis der Partner des GIDS-Projektes. Im einzelnen wird für jedes Szenario bewertet:

Wahrscheinlichkeit Diese Kategorie gibt unsere Einschätzung der Wahrscheinlichkeit wider, mit der der im Szenario beschriebene Schaden eintritt. Die Werte in der Tabelle sind: *sehr niedrig*, *niedrig*, *mittel*, *hoch* und *sehr hoch*.

Abwehr Gibt eine Einschätzung des Aufwands an, unter dem der Schaden abgewendet werden kann. Beispielsweise ist der Aufwand für den Schutz vor bekannten Angriffen relativ gering. Es ist ausreichend, die aktuellen Sicherheits-Updates einzuspielen. Es werden die Werte *sehr leicht*, *leicht*, *mittel*, *schwer* und *sehr schwer* verwendet.

Schaden Diese Kategorie wertet den entstandenen Schaden. So ist beispielsweise die Kompromittierung der Grid-Middleware kritischer als die Übernahme der Identität eines Grid-Benutzers. Werte sind wie bei der ersten Kategorie.

Risiko Gibt eine Einschätzung des Risikos wider, das sich aus den ersten drei Kategorien ergibt. Dabei steigt das Risiko mit Zunahme der Wahrscheinlichkeit, des Aufwands der Abwehr und des Schadens. Werte sind wie bei der ersten Kategorie.

Sensorik Für jedes Szenario sind verschiedene technische Sensoren relevant, über die Angriffe erkannt werden. Allerdings ist es nicht garantiert, dass immer eine Erkennung möglich ist. Beispielsweise kann die Übernahme der Identität eines Benutzers nicht direkt erkannt werden, wenn dieser das Passwort freiwillig weitergibt. In diesem Fall ist nur eine indirekte Erkennung durch nachfolgenden Missbrauch möglich.

Tabelle 4.1 listet die oben genannten Szenarien auf und zeigt die Bewertungen in den einzelnen Kategorien.

Szenario	Wahrscheinlichkeit	Abwehr	Schaden	Risiko	Sensorik
A1 - Viren und Würmer	sehr hoch	leicht	mittel	niedrig	NIDS Honeypot AV-Scanner
A2 - Kompromittierung Grid-Server / Middleware	niedrig	mittel	hoch	mittel	NIDS Host-IDS
A3 - Privilegieneskalation	niedrig	schwer	hoch	hoch	Host-IDS
A4 - Benutzer-Identität	hoch	schwer	mittel	hoch	System-Logs
A5 - Grid-IDS	niedrig	schwer	hoch	hoch	Netflow Host-IDS
A6 - Denial of Service	niedrig	leicht	mittel	niedrig	Netflow
M1 - Root-Kit	niedrig	schwer	mittel	mittel	Host-IDS RootKit-Scanner
M2 - Trojanisierte Software	mittel	mittel	sehr hoch	hoch	Host-IDS
M3 - Bot-Netze	niedrig	mittel	hoch	mittel	Netflow AV-Scanner
R1 - Missbrauch von Ressourcen	niedrig	schwer	niedrig	niedrig	System-Logs
R2 - Ausspähen von Informationen	niedrig	mittel	mittel	mittel	System-Logs
R3 - Manipulation von Ressourcen	niedrig	mittel	mittel	mittel	System-Logs Host-IDS
S1 - Verletzung der Grid-PKI	niedrig	mittel	hoch	mittel	
S2 - Zero-day Exploits	niedrig	schwer	hoch	hoch	Honeypot

Tabelle 4.1: Zusammenfassung der Bedrohungsszenarien, die Werte gehen von sehr niedrig, niedrig, mittel, hoch bis sehr hoch

4.6 Anforderungskatalog

In diesem Abschnitt werden die Anforderungen an das Grid-IDS abgeleitet, die sich aus den vorher eingeführten Bedrohungen ergeben. Die Anforderungen gliedern sich dabei in die folgenden Klassen und lassen sich wie folgt beschreiben:

- Anforderungen an die Sensorik zur Erkennung von Angriffen (Erkennungsleistung):

  Diversität: Die Auswertung der Szenarien hat gezeigt, dass kein Sensor alleine in der Lage ist, alle Angriffe zu erkennen.

- Funktionale Anforderungen an das Grid-IDS:

  Aussagekräftige Informationsaufbereitung: Aus der Komplexität der verschiedenen Szenarien folgt, dass nur durch die Kooperation der Sensoren der zusammenhängende Angriff rekonstruiert werden kann. Dies zieht die folgenden Punkte nach sich:

  - Aggregation und Korrelation der Daten, um dem Analysten alle unwichtigen Details auszublenden.
  - Bewertung und Priorisierung der Daten
  - Reduktion von False-Positives

  Aufgrund der Vielzahl der Daten, müssen diese zu sinnvollen Einheiten gruppiert werden können. Beispiel ist die Gruppierung von mehreren fehlgeschlagenen Login-Versuchen zu einem Passwort-Rateangriff.

  Mehrere einzelnd erkannte Angriffe werden durch Korrelation der Daten zu einem Angriff verschmolzen. Dies ermöglicht die Interpretierung des Angriffsziels. Die Korrelation ist insbesondere dann wichtig, wenn Schritte des Angriffs nicht durch die Sensorik erkannt werden können. Das kann beispielsweise die Übernahme eine Benutzeraccounts zum nachträglichen Missbrauch von Grid-Ressourcen sein. So ist es in diesem Fall wichtig, den Missbrauch zu erkennen und mit dem entsprecheneden Benutzeraccount oder der VO zu verbinden.

- Nichtfunktionale Anforderungen an das Grid-IDS:

  Interoperabilität der Sensoren: Die verschiedenen Typen von Sensoren müssen vom Grid-IDS koordiniert werden. Dies bildet die Grundlage, auf der die Aggregation und Korelation der Daten durchgeführt werden kann. Die technische Realisierung kann beispielsweise ein einheitliches Datenformat erfordern.

- Organisatorische Anforderungen:

  Weitergehende Kooperation: Die Erkennung von Angriffen ist nicht immer durch Sensorik möglich. Beispiel ist ein Benutzer, der sein Passwort durch Phishing weitergibt. Dies läßt sich nur indirekt feststellen, indem beispielsweise der Benutzer den Vorfall meldet. Dies setzt eine spezielle Seite voraus, die sich um die Sicherheit des Grids kümmert, beispielsweise ein Grid-CERT.

  Juristisch verwertbare Speicherung der Daten: Im Fall eines größeren Einbruchs in das Grid kann die Einleitung rechtlicher Schritte erwogen werden. Dies setzt voraus, dass die Daten zum Nachweis des Einbruchs und Verweis auf den Täter juristisch verwertbar gesichert werden. Neben den technischen Methoden zur Sicherung der Daten kann dies aber auch organisatorische nach sich ziehen - beispielsweise in Form einer Policy, welche Personen Zugriff zu den Daten oder Systemen haben.

- Sicherheitsanforderungen:

  Schutz der Grid-IDS Daten: Die Integrität, Authentizität, Vertraulichkeit und Verfügbarkeit der Daten des Grid-IDS müssen durch kryptographische Methoden geschützt werden.

Insgesamt decken sich diese Anforderungen mit den in Tabelle 3.20 zusammengefassten Anforderungen. Einzelne technische Anforderungen lassen sich aus den Eigenschaften der Sensoren und der Bearbeitung von Sicherheitsvorfällen ableiten. Jedoch sind diese in den abstrakten Anforderungen bereits enthalten.

Kapitel 5

Themenverwandte Arbeiten

5.1 Grid-basierte IDS

Seit ca. 2002 finden auch Intrusion Detection Systeme in und für Grids in der Forschung ihren Platz. Bei den meisten der Arbeiten lassen sich eine Reihe an Analogien zu konventionellen verteilten IDS feststellen, Grid-Spezifika hingegen werden meist stiefmütterlich behandelt. Nachfolgend werden eine Reihe an Ansätzen für Grid-basierte IDS kurz vorgestellt. Bei einigen Ansätzen bleibt es dabei nur bei einem Konzept, zu dem leider keine (prototypische) Implementierung gefunden werden kann, einige Entwicklungen hingegen können auch mit einem Prototypen aufwarten. Die Reihenfolge der Vorstellungen orientiert sich aufsteigend nach dem Jahr der ersten Veröffentlichung der entsprechenden Arbeit.

5.1.1 Grid-Based Intrusion Detection System (GIDS)

Bereits 2003 ist in [7] das *Grid-based Intrusion Detection System* (GIDS) vorgestellt worden. Dieser Vorschlag stellt eines der ersten Intrusion Detection Systeme für Grid-Umgebungen in der Forschung dar. Erstmals wird der VO-Aspekt in einem Intrusion Detection System aufgebracht. Vielmehr noch wird das GIDS selbst als eine VO modelliert, welche den Dienst des Grid-basierten IDS für andere VOs im Grid anbietet.
Als Anforderungen an das GIDS spezifizieren die beiden Autoren ...

1. den Umgang des GIDS mit der Grid-Umgebung (insbesondere dem Teilen von Ressourcen und der Kollaboration von Nutzern und Diensten),
2. die Autonomie des GIDS, so dass der Anwender und Administrator möglichst wenig interagieren müssen,
3. die Flexibilität des GIDS, insbesondere im Hinblick auf die nutzerspezifische Systemanpassungen und den Einsatz von Policy-Rahmenwerken,
4. Skalierbarkeit,
5. Wiederverwendbarkeit,
6. Erweiterbarkeit,
7. einen geringen Overhead, so dass das GIDS die Performanz des Grids nicht maßgeblich beeinflusst,
8. eine zeitnahe Auswertung von Angriffsberichten.

Abbildung 5.1 stellt schematisch nach der Arbeit in [7] die Idee zum Aufbau des GIDS dar. Es folgt eine sehr wenig detaillierte Beschreibung des GIDS, vielmehr wird postuliert, dass eine Vielzahl verschiedener Auswertungsmechanismen und ein Policy-Based Management Ansatz

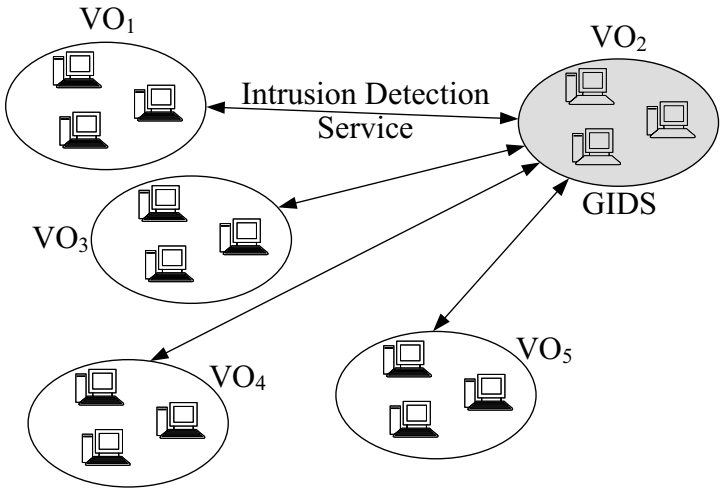

Abbildung 5.1: Grid-Based Intrusion Detection System (GIDS) nach [7]

zur Zugriffskontrolle zum Einsatz kommen kann, wobei das System für auf dem Globus Toolkit basierende Grids gedacht ist. Jedoch bewegt sich jegliche Beschreibung auf einem groben Niveau, vielmehr werden alleinstehend Schlagworte zur Datenanalyse in konventionellen Intrusion Detection Systemen benannt, diese aber nicht weiter verfolgt. Zur Sammlung einer Informationsbasis, auf der das GIDS arbeiten kann, wird nichts weiter verlautet. Weiter nachteilig erscheint, dass eine Angriffanalyse zentralisiert vorgenommen wird und seit 2003 eine Implementierung hierzu aussteht. Zusammenfassend wird der Vorschlag dieses GIDS als „Backup“ der *Grid Security Infrastructure* (GSI) bezeichnet, wobei aber die GSI keine Frühwarnmechanismen vorsieht.

Zusammenfassung:

- Bringt VO-Aspekt auf
- Ist selbst als VO modelliert
- Bietet IDS-Dienst im Grid an
- Erkennbare Angriffstypen:
  - Der Ansatz fokussiert auf das Auditing des Globus Toolkit, Log-File Überwachung, Anomalieerkennung und signatur-basierte Missbrauchserkennung.
  - Das Konzept sieht jedoch eine Angriffserkennung mit beliebiger Analysefunktion vor, deswegen sind prinzipiell alle Angriffstypen erkennbar.
- Nachteile:
  - Einzig für das Globus Toolkit gedacht
  - Informationssammlung zur Angriffserkennung nicht berücksichtigt
  - Zentralisierte Angriffsanalyse
  - Keine Implementierung seit 2003

5.1.2 Grid Intrusion Detection Architecture (GIDA)

Die beiden Arbeiten [47] und [48] präsentieren den Ansatz der *Grid Intrusion Detection Architecture* (GIDA). Abbildung 5.2 stellt den schematischen Aufbau nach [47, 48] der GIDA dar. Die Autoren beschreiben für ihr System dabei die zwei zentralen Bestandteile des *Intrusion*

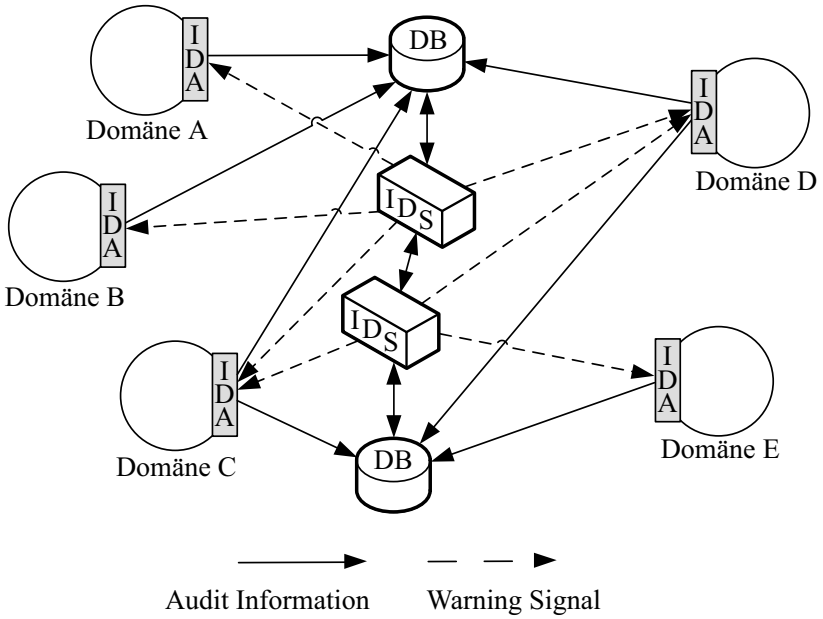

Abbildung 5.2: Grid Intrusion Detection Architecture (GIDA) nach [47, 48]

Detection Agent (IDA) und des *Intrusion Detection Server* (hier mit IDS abgekürzt!). Ein IDA ist in dieser Architektur dafür verantwortlich, Informationen für die GIDA zu sammeln, während sich der Intrusion Detection Server für die Auswertung der gesammelten Informationen verantwortlich zeichnet. Dabei ist eine nicht weiter beschriebene Kooperation der Server untereinander vorgesehen.
Bei der Konzeption der GIDA standen insgesamt sechs Anforderungen im Vordergrund:

1. Der Umgang der GIDA mit der Heterogenität im Grid
2. Skalierbarkeit
3. Umgang mit der Dynamik im Grid und Fehlertoleranz der GIDA
4. Keine zentralisierte Kontrolle
5. Die Nutzung von Standards, zum Beispiel im Hinblick auf Protokolle
6. Nicht-triviale Auswertungsanalyse und die Unterstützung verschiedener Vertrauensbeziehungen

Bei der GIDA handelt es sich um ein verteiltes Gesamtsystem unter Nutzung eines Peer-to-Peer Ansatzes. Für die Angriffserkennung wird eine vollständige Informationsreplikation gewährleistet, die zusätzlich zu einer erhöhten Ausfallsicherheit beitragen soll. Als Analysefunktion soll ein Anomalieerkennungsverfahren zum Einsatz kommen, andere Angriffserkennungen sind derweil nicht vorgesehen. Es existiert eine prototypische Implementierung zur GIDA, die auf simulierten Grid-Infrastrukturen basiert und ein Anomalieerkennungsverfahren unter der Nutzung von *Learning Vector Quantization* (LVQ) als Spezialfall eines künstlichen Neuronalen Netzes implementiert. Allerdings setzt dieses System eine homogene Infrastruktur voraus, eine Erweiterung auf heterogene Umfelder ist noch ausstehend. Außerdem führt eine Variation der Teilnehmerzahl am IDS zu einer enormen Rate an Fehlalarmen und sämtliche VO-Aspekte im Grid bleiben unberücksichtigt.

Zusammenfassung:

- Verteiltes System, P2P Ansatz

- Vollständige Informationsreplikation
- Erkennbare Angriffstypen:
  - Als Auswertungslogik wird ein Anomalieerkennungsverfahren vorgeschlagen.
  - Die Analysefunktion ist prinzipiell beliebig, auch wenn dies nicht explizit durch die Autoren erwähnt wird.
  - Mit leichten Anpassungen sind vom Konzept her beliebige Angriffe erkennbar.
- Nachteile:
  - Erweiterung auf heterogene Umfelder ausstehend
  - Variation der Teilnehmerzahl führt zu enormer Fehlalarmrate
  - VO-Aspekt unberücksichtigt
  - Es kommen ausschließlich Anomalieerkennungsverfahren zur Angriffserkennung zum Einsatz

5.1.3 Performance-based Grid Intrusion Detection System (PGIDS)

In den Arbeiten von Leu et. al. [30, 31] wird das *Performance-based Grid Intrusion Detection System* (PGIDS) vorgestellt. Dabei werden die Grid-Knoten als Analyseeinheiten eingesetzt, was eine nennenswert abweichende Vorgehensweise im Vergleich zu anderen Ansätzen darstellt. Insbesondere kann durch diesen Ansatz eine Lastverteilung, wenn auch zum Preis der zusätzlichen Belastung der verfügbaren Ressourcen im Grid, realisiert werden.

Das PGIDS besteht im wesentlichen aus den Komponenten *Dispatcher*, *Scheduler*, *Detection Nodes* (DN) und *Block List Database* (BLD). Als Annahme gilt, dass an einem PGIDS mehrere Subnetze beteiligt sind, die alle derselben *Network Management Unit* (NMU) und somit der gleichen administrativen Domäne angehören. Ein jedes Subnetz erhält einen Dispatcher, der unter Nutzung des Spiegel-Ports seines zentralen Switches Flow-Daten aufzeichnet, die in sogenannten *Flow Files* (FF) abgelegt werden. Diese Dateien werden via GridFTP als Grid-Job zur Analyse verarbeitet. Der Scheduler ist dafür verantwortlich, dass ein geeigneter DN für die Analyse eines jeden FF ausgewählt wird. Die Ergebnisse der Analyse, also potentiell erkannte Angriffe, werden mit Informationen zu Zeit, Quell- und Zieladresse, Protokoll und Angriffstyp in der BLD hinterlegt. Diese Daten dienen dann dazu, Firewalls zu rekonfigurieren, um Angreifer effektiv vom Grid fernzuhalten.

Die Nachteile dieses Systems sind vor allem, dass es durch den zentralen Scheduler einen Single-Point-of-Failure bietet und ein vollständiges Vertrauen unterhalb der Teilnehmer voraussetzt. Zudem ist das System konstruktionsbedingt nur in der Lage, unter Nutzung der Grid-Ressourcen netzbasierte Angriffe zu erkennen. Zudem werden nur Angriffe, die außerhalb des Grids ihren Ursprung finden, betrachtet, interne Angriffe hingegen bleiben unerkannt.

Zusammenfassung:

- Grid-Knoten als Analyseeinheiten
- Autonomes PGIDS je Partei
- Zentraler Scheduler je PGIDS
- Erkennbare Angriffstypen:
  - Laut Autoren sind Denial-of-Service Angriffe, verteilte DoS und Angriffe durch die Ausnutzung bestehender Schwachstellen in Software-Komponenten erkennbar.
  - Die Angriffserkennung erfolgt unter Nutzung Neuronaler Netze. Wenn auch nicht explizit erwähnt, scheint das Erkennungsverfahren jedoch austauschbar.
  - PGIDS erkennt durch seinen Aufbau bedingt (das heißt durch die geforderte Sensorplatzierung) nur netzbasierte Angriffe.

- Nachteile:
  - Erkennt nur netzbasierte Angriffe
  - Single-Points-of-Failure
  - Setzt vollständiges Vertrauen unter Teilnehmern voraus
  - Basiert ausschließlich auf dem Globus Toolkit als Middleware
  - Kann nur externe Angriffe erkennen

5.1.4 GridSec

In einer aus dem Projekt *GridSec* resultierenden Arbeit „Trusted Grid Computing with Security Binding and Self-Defense against Network Worms and DDoS Attacks“ [20] wird eine Sicherheitsinfrastruktur vorgestellt, die Selbstverteidigungsmechanismen in Grid-Umgebungen zur Verfügung stellt. Dabei fokussiert das System auf die Abwendung von netzbasierten Angriffen, die durch Würmer initiiert sind, und das Verhindern verteilter Denial-of-Service Angriffe.

Architekturell orientiert sich das System an einem verteilten IDS, das durch ein Overlay-Netz die teilnehmenden Partner untereinander verbindet. Mit Hilfe dieses Netzes können Informationen zu Angriffen, die ein je Partner autonomes IDS generiert, unter Gewährleistung der Vertraulichkeit und Integrität ausgetauscht werden. Um die Vertrauenswürdigkeit eines angeschlossenen IDS zu bewerten, wird eine Methode vorgeschlagen, die aus verschiedenen Parametern zur Effizienz des IDS (zum Beispiel Erfolgsrate, Auslastung etc.) aus historischen Daten einen sogenannten *Trust Index* (TI) eines jeden IDS bildet, wozu Ansätze aus der Fuzzy-Logic herangezogen werden.

Zusätzlich zur Erkennung von Angriffen durch die lokalen IDS-Instanzen wird eine globale Aggregation und Korrelation der Daten vorgenommen. Hierdurch wird das Ziel verfolgt, weit verteilte Angriffe effizienter erkennen zu können.

Neben der reinen Erkennung von aktiven Würmern und verteilten Denial-of-Service Angriffen steht auch ein Maßnahmenkatalog zur aktiven Abwehr erkannter Angriffe zur Verfügung. Das Einleiten von Gegenmaßnahmen wird dabei in Form von Verbindungsunterbrechungen vorgeschlagen.

Zusammenfassung:

- Verteiltes IDS
- Autonome, lokale IDS-Instanzen werden Grid-global zusammengeführt
- Lokal erkannte Angriffe werden Grid-global korreliert
- Gegenmaßnahmen in Form von Verbindungsunterbrechungen dienen als Verteidigungsmechanismen
- Erkennbare Angriffstypen:
  - Netzbasierte Würmer
  - Verteile Denial-of-Service Angriffe
- Nachteile:
  - Erkennt nur aktive Würmer und verteilte Denial-of-Service Angriffe
  - Keine Mechanismen zur Berichterstattung (Reporting)
  - Berücksichtigt keine VO-Aspekte

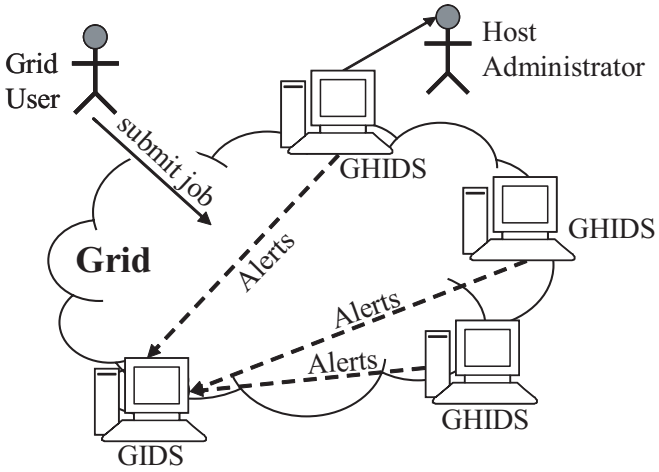

Abbildung 5.3: Architekturüberblick des GHIDS nach [10]

5.1.5 Grid-specific Host-based Intrusion Detection System (GHIDS)

Feng et. al. entwickeln in ihrer Arbeit das *Grid-specific Host-based Intrusion Detection System* (GHIDS) [10]. Der Ausgangsgedanke dieser Arbeit ist, dass herkömmliche Host-basierte IDS (HIDS) nicht in der Lage sind, Grid-spezifische Angriffe zu erkennen und keine Grid-Spezifika (beispielsweise den Grid-Nutzer) kennen. Daraus resultiert die Idee, dass lokale Instanzen eines IDS die Aktionen der Grid-Anwender überwachen sollen und die daraus gewonnenen Berichte Grid-global korreliert werden. Dazu kommt eine angepasste Variante eines HIDS zum Tragen, die in der Lage ist, lokale Nutzerkennungen auf Kennungen im Grid abzubilden, so dass eine Korrelation im Grid ermöglicht wird. Diese Instanzen werden im Rahmen der Arbeit als *Grid-based HIDS* oder kurz *GHIDS* bezeichnet. Die von jedem GHIDS generierten Berichte und Alarme werden an ein *Grid-based IDS* (GIDS) weitergereicht, welches deren Korrelation Grid-global vornimmt. Zusätzlich können lokal generierte Alarme natürlich auch an einen lokal verantwortlichen Administrator übermittelt werden. Abbildung 5.3 illustriert das Konzept nochmals.

Zusammenfassung:

- Lokale HIDS werden um das Wissen von Grid-Nutzern erweitert
- Lokal erzeugte Alarme werden Grid-global korreliert
- Erkennbare Angriffstypen:
  - Dieser Ansatz erweitert hostbasierte IDS um das Wissen von Grid-Nutzeridentitäten.
  - Die Sensorplatzierung ist auf mit dem GHIDS ausgestatteten Grid-Rechner beschränkt.
  - Dadurch ist das GHIDS erstmal beschränkt auf die Erkennung hostbasierter Angriffe, durch eine Korrelation können noch gewisse Rückschlüsse auf verteile Angriffe gezogen werden.
- Nachteile:
  - Sehr eingeschränkter Erkennungsfokus durch die Basis von HIDS
  - Insbesondere können netzbasierte Angriffe nur sehr eingeschränkt erkannt werden
  - Volles Vertrauen unter den Teilnehmern ist implizit und notwendig
  - VO-Aspekte bleiben vollkommen unberücksichtigt
  - Der Datenschutz wird nicht weiter betrachtet, Informationen werden ungefiltert weitergereicht

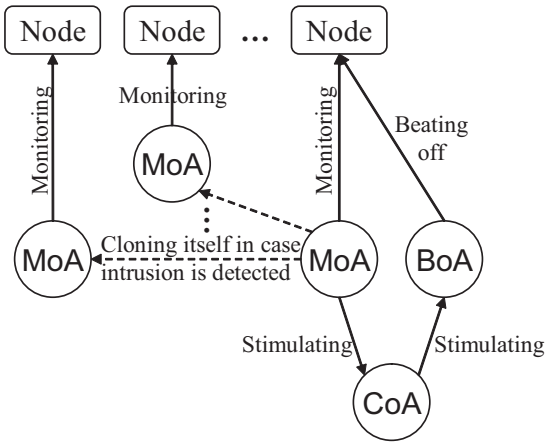

Abbildung 5.4: Das Intrusion Detection Modell der GIDIA nach [14]

5.1.6 Grid Intrusion Detection Based on Immune Agent (GIDIA)

Eine zu allen anderen hier präsentierten Ansätzen vollkommen konträre Idee wird in [14] vorgestellt. Gong et. al. stellen ein Intrusion Detection System vor, das sich das Konzept eines künstlichen Immunsystems zu Nutze macht. Abbildung 5.4 illustriert das Intrusion Detection Modell, welches der GIDIA zu Grunde liegt.

Sogenannte *Antigene* werden als Eigenschaften von Grid-Diensten spezifiziert und von *Monitoring Agents* (MoA) überwacht. Die Antigene teilen sich dabei in Eigenschaften auf, die der Anwender-, System-, Prozess- oder Paketebene zuordnen lassen. Innerhalb der MoAs wird auf Basis der erhobenen Monitoring-Informationen eine Einbruchserkennung durchgeführt. Sollte ein Angriff erfolgreich erkannt werden, so werden die sogenannten *Beating Off Agents* (BoA) stimuliert und mit möglichst detaillierten Informationen zu einem erkannten Angriff versorgt. Die BoAs reagieren nachfolgend auf den Angriff, wodurch das GIDIA nicht nur über einen Erkennungsmechanismus, sondern auch über eine Einheit zur Ausführung geeigneter Gegenmaßnahmen verfügt. Durch *Communicator Agents* (CoA) wird die Kommunikation unterhalb der Agenten sichergestellt und gewährleistet.

In [34] wird im Jahre 2007 das *Self-adaptive Intrusion Detection System for Computational Grids* als auf das GIDIA aufbauendes System präsentiert. Es basiert primär auf den von der Grid Security Infrastructure bereitgestellten Diensten und bildet eine hierarchische Struktur von Agenten. Das Grid-basierte IDS wird anhand sogenannter *Trust Communities* (TC) unterteilt, die jeweils dynamisch als VO kreiert werden. Eine jede Trust Community kann selbstständig eine Angriffserkennung durchführen und nach Beschluss eines *Decision-Making Module* (DMM) unter Nutzung des *Response Module* (RM) auf einen erkannten Angriff reagieren.

Zusammenfassung:

- Idee eines künstlichen Immunsystems
- Monitoring Agenten überwachen einzelne Grid-Knoten
- Verteidigungsmechanismen durch Beating Off Agents
- Erkennbare Angriffstypen:
  - Die GIDIA nutzt einzig ein nicht änderbares oder erweiterbares Angriffserkennungsverfahren basierend auf einem künstlichen Immunsystem.
  - Die Platzierung der Sensoren ist auf die „Nodes“ beschränkt.
  - Daraus folgend werden diverse Angriffe aus allen Angriffsklassen nicht oder falsch erkannt werden.

- Nachteile:
  - Erkennungsfunktion nicht änderbar, zum Beispiel keine signaturbasierte Analyse möglich
  - Durch eingeschränkte Sicht der MoAs und mangelnde Grid-globale Korrelation sind weit verbreitet angelegte Angriffe nur sehr schwer erkennbar
  - Der Datenschutz wird nicht weiter beachtet
  - Totale Kontrolle und absolutes Vertrauen ist Grundvoraussetzung für das GIDIA

5.1.7 Grid intrusion detection based on soft computing (SCGIDS)

In einem ähnlichen Ansatz zur zuvor erwähnten GIDIA versucht das *Grid intrusion detection based on soft computing* (SCGIDS) [52] das Normalverhalten eines Grid-Nutzer in einem neuronalen Netz zu modellieren und Abweichungen davon festzustellen, die berichtet werden können. Die Arbeit baut auf eine Vorarbeit von Kenny und Coghlan auf [25] und erweitert diese um den Ansatz des Soft Computing.

Das SCGIDS verfügt über eine Reihe von Agenten (die sogenannten *SCGIDA*s, deren Abkürzung leider nicht expandiert wird), die das Nutzerverhalten der Grid-Nutzer, die zurzeit im Grid aktiv sind, beobachten und aufzeichnen. Zudem tauschen sie ihre Beobachtungen untereinander aus, um so jeder für sich eine Grid-weite Erkennung von Abweichungen in Bezug auf das zuvor festgestellte Normalverhalten durchzuführen. Diese Abweichungen werden durch das SCGIDS als Angriff interpretiert.

Ein SCGIDA besteht im Wesentlichen aus drei Datenbanken, der *Signature Identification Database* (SIDB), der *User Behavior Model Parameter Database* (UBMPDB) und der *Intrusion Evidence Database* (IEDB), sowie insgesamt acht weiteren Komponenten. Ein *Sniffing Agent* (SA) zeichnet Informationen des Grid-Nutzerverhaltens auf, die durch den *Signature Match Agent* (SMA) gegen die SIDB abgeglichen werden. Liegt kein Treffer vor, so wird ein Angriff antizipiert. Im Falle eines Treffers wird das erkannte Nutzerverhalten aus der UBMPDB in die UBMA transferiert. Nachfolgend kommt ein Neuronales Netz zum Einsatz, das unter Nutzung der aktualisierten UBMA die aktuellen Nutzungsprofile der Grid-Anwender auf ihre Normalität hin klassifiziert und die Parameter des Modells anpasst. Sollte hierbei ein abnormales Nutzerverhalten auffallen, kommt der *Trace-Back and Response Agent* (TBRA) zum Einsatz, der das abnormale Nutzerverhalten nachverfolgt und möglichst detailliertes Beweismaterial in der IEDB hinterlegt. Zur Interkommunikation der SCGIDAs kommt ein *Communication Agent* (CA) zum Einsatz, ein gewisser Selbstschutz des Systems wird durch den *Self Protection Agent* (SPA) durch regelmäßige Statusabfragen eines jeden Agenten realisiert.

Zusammenfassung:

- Basiert auf einer Vorarbeit, dem *Grid-wide Intrusion Detection* [25]
- Erweitert diesen Ansatz um Konzepte des Soft Computing unter Nutzung eines Neuronalen Netzes
- Kann in gewisser Art Beweise zu Angriffen für forensische Zwecke zur Verfügung stellen
- Erkennbare Angriffstypen:
  - Das SCGIDS einzig ein nicht änderbares oder erweiterbares Angriffserkennungsverfahren basierend auf Neuronalen Netzen und Ansätzen der Fuzzy-Logic.
  - Es wird versucht Abweichungen im Verhalten einzelner Nutzer zu erkennen.
  - Andere Angriffstypen sind nicht im Fokus des SCGIDS.
- Nachteile:
  - Erkennungsfunktion nicht änderbar, zum Beispiel keine signaturbasierte Analyse möglich

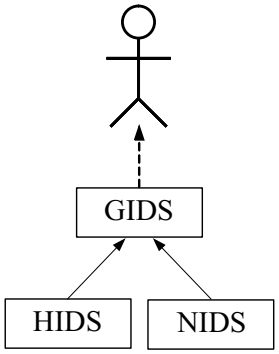

Abbildung 5.5: Integrated Grid-based Intrusion Detection System nach [40, 39]

- Der Datenschutz wird nicht weiter beachtet
- Absolutes Vertrauen unter den Agenten ist Grundvoraussetzung
- Stellt eher ein verteiltes IDS dar, spricht keine Grid-Spezifika an

5.1.8 Integrated Grid-based Intrusion Detection System

In einer Arbeit der Universität von Santa Catarina (Brasilien) wird das *Integrated Grid-based Intrusion Detection System* vorgestellt [40, 39]. Dieses System fokussiert auf die Erkennung unerlaubter Zugriffe, missbräuchlicher Nutzung von Grid-Ressourcen, Exploits und host- oder netzspezifische Angriffe. Als generelle Unterschiede zwischen Angriffen auf Grids und solchen auf herkömmliche verteilte Systeme werden lediglich die zu erwartende höhere Geschwindigkeit und das aller Voraussicht nach größere Schadenspotenzial angesehen.

Die Grundidee ist ein übergeordnetes System zu entwickeln, das eine Zusammenführung von host- und netzbasierten IDS vorsieht, wie Abbildung 5.5 aus [40] und [39] darstellt. Auf diese Weise lassen sich übergreifend sicherheitskritische Vorfälle ableiten, um dann gegebenenfalls Alarmmeldungen generieren zu können. Der Datenaustausch geschieht unter Nutzung des XML-basierten Intrusion Detection Message Exchange Format (IDMEF).

Für die Umsetzung dieses Ansatzes wird eine abstrakte, dreigeteilte Architektur entwickelt, die sich auf Agenten, Analysekomponenten und eine Steuereinheit stützt. Agenten greifen die sicherheitsrelevanten Informationen der einzubindenden Intrusion Detection Systemen ab und speichern sie in Datenbanken im Grid. Jeder Zugriff eines Anwenders initiiert eine Überprüfung gegen das in der Datenbank gespeicherte Nutzerprofil. Sollten übermäßige Abweichungen zwischen einem aufgezeichneten Nutzerprofil und dessen tatsächlichem Verhalten auffallen, so wird eine weitergehende Analyse an Knoten des Grids mit freien Rechenkapazitäten vergeben, die ihrerseits mit den Datenbanken kommunizieren und gegebenenfalls Profile aktualisieren. Zusätzlich zur Analyse von Nutzerprofilen kann ebenfalls eine Aggregation und Korrelation gespeicherter sicherheitsrelevanter Ereignisse durchgeführt werden um so verteilte Angriffe identifizieren zu können.

Die Weiterentwicklung dieses Ansatzes ist noch immer im Gange, aktuelle Arbeiten wie [42] befassen sich nach wie vor mit diesem System, dessen Entwicklung und Tests seiner Leistungsfähigkeit.

Zusammenfassung:

- Übergeordnetes System zu bestehenden HIDS und NIDS
- Datenaustausch IDMEF-basiert (XML)
- Speichert Informationen in DBs im Grid
- Erkennbare Angriffstypen:

  - Durch die Kombination von host- und netzbasierten IDS sind vom Konzept alle Angriffstypen erkennbar.
  - Die Arbeit beschränkt sich jedoch auf die Erkennung unerlaubter Zugriffe, missbräuchlicher Nutzung von Grid-Ressourcen, Exploits und host- oder netzspezifische Angriffe.

- Nachteile:
  - Zentralisierter Aufbau
  - Grid-Aspekte unberücksichtigt – es handelt sich eher um ein verteiltes IDS
  - Der Datenschutz wird nicht weiter beachtet
  - Volles Vertrauen unter den Teilnehmern ist implizit und notwendig
  - VO-Aspekte bleiben vollkommen unberücksichtigt

5.2 Implementierungen und Produkte im Bereich GIDS

An dieser Stelle sollen einige für die Realisierung des GIDS-Dienstes relevante Produkte und Implementierungen genauer betrachtet werden. Hierzu zählen neben kommerziellen und etablierten Produkten namhafter Firmen auch eine Vielzahl von Open-source-Projekten / Produkten. Ziel dieses Abschnitts ist es, vorhandene Produkte und Ansätze miteinander zu vergleichen, jeweilige Vor- und Nachteile zu bestimmen und herauszuarbeiten, welche Anforderungen an ein Grid-basiertes Intrusion Detection System von keinem der auf dem Markt vorhandenen Produkte erfüllt werden können.

5.2.1 StoneGate™ - Intrusion Prevention System

Die Firma Stonesoft bietet mit ihrem Intrusion Detection/Prevention System StoneGate™ ein Produkt an, mit welchem mittlere und große Netzwerke gegen zahlreiche Angriffe geschützt werden können. StoneGate™ bietet durch seinen modularen Aufbau die Möglichkeit, sowohl virtuelle als auch physikalische Netzwerkumgebungen zu sichern. Das IPS ist in der Lage eine Vielzahl von Angriffen zu erkennen. Hierzu zählen unter anderem Angriffe, wie Buffer Overflows, Würmer, Trojaner, Spyware, DoS- und DDoS-Attacken, Backdoors und anderen verdächtigen Netzwerkverkehr. Wird ein Angriff durch StoneGate™ erkannt, so stehen die für ein Prevention-System üblichen reaktiven Maßnahmen, wie das Terminieren oder Zulassen von Verbindungen, das Loggen und Alarmieren, sowie die Möglichkeit, den folgenden Netzwerkverkehr aufzuzeichnen, zur Verfügung.

Eines der wesentlichen Verfahren eines Intrusion Detection Systems, um Angriffe sicher erkennen zu können, ist der Vergleich von aktuellem Netzwerkverkehr mit bereits bekannten Signaturen von Angriffen. StoneGate™ bietet hier über 3000 solche Signaturen für über 160 Protokolle. Ebenso werden Netzwerkprotokolle wie P2P, Instant Messaging, sowie Streaming- und Tunneling-Protokolle erkannt und können kontrolliert werden. Neben dem Vergleich von bereits bekannten Angriffsmustern zeichnen sich Intrusion Detection/Prevention Systeme durch ihre Fähigkeit aus, auch unbekannte Angriffe durch statistische Analysen aufdecken zu können. StoneGate™ bietet hierfür die Attack Sequence Detection, die mit Hilfe eines verbesserten Moduls zur Ereigniskorrelation auch Angriffe erkennen kann, die noch nicht zu einem effektiven Eindringen in das Netzwerk geführt haben. Es können also entsprechend auch komplexe Angriffversuche erkannt und entsprechend im Folgenden zuverlässig wiedererkannt werden.

StoneGate™ bietet ebenfalls die Möglichkeit, vorhandene Netzwerke einer bestehenden Infrastruktur in Sicherheitszonen aufteilen zu können. Auf diese Weise lassen sich verschiedene sicherheitskritische Bereiche eines Netzwerks voneinander trennen und die Gefahr der Infektion und des Missbrauchs von ganzen Netzwerken minimieren. Ein großer Vorteil gegenüber anderen Systemen besteht darin, dass die Segmentierung des bestehenden Netzwerks in die entsprechenden Sicherheitszonen keine Änderung der Netzwerkkonfiguration voraussetzt.

Zusammenfassung

- Kommerzielles Intrusion Prevention System
- Möglichkeit der Bildung von Sicherheitszone
- Erkennbare Angriffstypen:
  - Bekannte Angriffe mittels Pattern Recognition
  - Unbekannte Angriffe mittels statistischer Analysen und Attack Sequence Detection
- Nachteile:
  - Vergleichsweise hohe Anschaffungskosten
  - Keine genauen Informationen über interne Funktionsweise
  - Autonomie der beteiligten Ressourcenanbieter kann nicht gewährleistet werden (Informationsanonymisierung / Datenschutz / keine zentrale Beschaffungsverfügung im D-Grid)
  - Zielsetzung auf Unternehmensnetze, daher keine native D-Grid-Eignung

5.2.2 Cisco Adaptive Security Appliance

Als Beispiel für ein Intrusion Detection und Prevention System aus dem Hause Cisco wird an dieser Stelle die 5500er Serie der Adaptive Security Appliance (ASA) betrachtet. Hierbei handelt es sich um eine integrierte Gesamtlösung, die neben dem eigentlichen IPS auch eine Firewall und eine VPN-Lösung beherbergt. Mit Hilfe dieser Kombination kann auch dieses Intrusion Prevention System verschiedenste Angriffe, wie beispielsweise Würmer, Trojaner, Viren, DoS und DDoS-Attacken, sowie Angriffe gegen Betriebssysteme und Anwendungen, erkennen und abwehren. Auch die genaue Kontrolle über erlaubte und nicht zulässige Anwendungen im Netzwerk und die Erkennung von infizierten Dateianhängen wird ermöglicht.

Einen Vorteil gegenüber vielen anderen Produkten hat Cisco bei der Auswertung und Bereitstellung von Signaturen-Updates. Für das Global Correlation genannte Verfahren, stellt Cisco eine große Infrastruktur bereit, die es ermöglicht alle ASAs alle 5 Minuten auf den neuesten Stand zu bringen. So werden alle Systeme nahezu in Echtzeit mit den aktuellsten Signaturen neuer Angriffe und anderen Updates versorgt.

Neben dem Vergleich von Bestandsignaturen mit aktuellen bietet die 5500er-Serie der ASA ebenso statistische Analysen. Hiermit sollen Zero-Day-Attacken verhindert werden. Während einer Lernphase ermittelt das System das Normalverhalten im Netzwerk und kann im Anschluss daran ein Fehlverhalten aufgrund von Angriffen erkennen und verhindern. Hierfür müssen im Gegensatz zum Vergleichsverfahren keine Signaturen alter Angriffe vorhanden sein.

Zusammenfassung

- Kommerzielles Intrusion Prevention System
- Global Correlation und Updates alle 5 Minuten
- Erkennbare Angriffstypen:
  - Bekannte Angriffe mittels Pattern Recognition
  - Unbekannte Angriffe / Zero-Day-Attacken
- Nachteile:
  - Vergleichsweise hohe Anschaffungskosten
  - Keine Informationen über interne Funktionsweise
  - Autonomie der beteiligten Ressourcenanbieter kann nicht gewährleistet werden (Informationsanonymisierung / Datenschutz / keine zentrale Beschaffungsverfügung im D-Grid)
  - Zielsetzung auf Unternehmensnetze, daher keine native D-Grid-Eignung

5.2.3 Lancope StealthWatch

Lancope StealthWatch ist ein Intrusion Detection und Prevention System, dass Daten von NetFlow, sFlow, syslog und SNMP zur Erkennung von Angriffen verwendet. Weiterhin werden Aktionen der Benutzer überwacht. Aufbauend auf den Netflow Daten werden statistische Werte für legitimen Netzwerkverkehr (*Baseline*) berechnet. Angriffe werden an signifikanten Abweichungen zu der Baseline erkannt. Laut Angaben in [29] ermöglicht dies unter anderem die Erkennung unbekannte Angriffe, Bot-Netzwerke und Denial of Service Angriffe.

Eine weitere Anwendung sind Verletzungen einer Sicherheitspolicy. Diese kann beispielsweise durch Peer-to-Peer Netzwerkverkehr oder die nicht-autorisierte Installation einer Anwendung entstanden sein. Analog zu CarmentiS werden die Angriffe und Sensordaten an einer zentralen Stelle gesammelt und durch eine Web-Anwendung dargestellt.

Zusammenfassung

- Kommenzielles verhaltensbasiertes IDS
- Lancope StealthWatch ist ein Frühwarnsystem, das im wesentlichen auf Netflow-Daten basiert
- Auswertung der Daten in der zentralen Management Konsole
- Erkennbare Angriffstypen:
  - Alle Angriffe, die sich von der Baseline unterscheiden[1]
- Nachteile:
  - Wenig technische Informationen
  - Konzept des Frühwarnsystems nicht direkt auf das Grid-IDS übertragbar
  - Autonomie der beteiligten Ressourcenanbieter kann nicht gewährleistet werden (Informationsanonymisierung / Datenschutz / keine zentrale Beschaffungsverfügung im D-Grid)

5.2.4 Snort IDS

Snort [43] ist ein signaturbasiertes Intrusion Detection System, das unter einer GPL-Lizenz (GNU General Public License) verfügbar ist. Für die Erkennung eines Angriffs auf eine bestimmte Schwachstelle wird nach einem charakteristischen Muster gesucht, das dann die Grundlage der Signatur bildet. Neben den Signaturen gibt es Module zur Erkennung von Angriffen, die nicht als Signatur abgebildet werden können. Dies betrifft beispielsweise Portscans.

Einfachste Möglichkeit ist die Anwendung der Signaturen auf einzelne Netzwerkpakete. Dies funktioniert allerdings nicht, falls sich der Angriff auf mehrere Pakete verteilt. Daneben kann ein Angreifer bewußt die Daten auf mehrere Pakete verteilen, um den Angriff zu verschleiern. Analoges gilt für fragmentierte IP-Pakete. Als Reaktion wurden in Snort mehrere Präprozessoren (*Preprocessors*) eigeführt, die Netzwerk-Pakete im Rahmen der TCP/IP Protokollfamilie zu einem Datenstrom zusammenfügen. Desweiteren existieren mehrere Präprozessoren zur Beabeitung von höheren Protokollen wie FTP, HTTP, SMTP und SSH.

Der wichtigste Bestandteil der Signaturen sind die Muster zur Charakterisierung des Angriffs. Da es häufig unterschiedliche Wege gibt, eine Schwachstelle auszunutzen, wird versucht, die Signatur auf die Schwachstelle anzupassen. Dies verhindert, dass nur einzelne Exploits aber nicht deren Varianten erkannt werden. Die Signaturen beinhalten in der Regel ein oder mehrere Paare von jeweils einem Offset und entweder einer festen Zeichenkette oder eines regulären Ausdruckes. Jedes dieser Muster wird auf die Daten einer Netzwerkverbindung angewendet und trifft dann zu, wenn die Zeichenkette an der Position des Offsets vorhanden ist oder der

[1] Vom Hersteller werden nur wenige Informationen über die Funktionsweise öffentlich bereit gestellt.

reguläre Ausdruck an dieser Stelle zutrifft.

Vorteil der Netzwerk-basierten IDS ist, dass diese an einer zentralen Stelle im Netzwerk positioniert werden können. Beispielsweise kann ein IDS hinter dem zentralen Router den vollständigen Netzwerkverkehr ein- und ausgehend überwachen. Dabei muss das NIDS bei Änderungen im Netzwerk nicht unkonfiguriert werden. Sie haben aber vom Prinzip bedingt mehrere Nachteile. Weil für unbekannte Angriffe keine Signaturen existieren, können diese nur durch Zufall erkannt werden - beispielsweise, wenn eine Signatur für einen verwandten Angriff zutrifft. Desweiteren sehen sie nur die rohen Verbindungsdaten. Dies verhindert einen effektiven Einsatz für verschlüsselte Verbindungen. Da NIDS keine internen Zustände der angegriffenen Systeme überwachen können, geben diese nur eingeschränkt Informationen über den Erfolg des Angriffs. Ein weiterer Nachteil von Snort ist, dass Zustände bei Protokollen nur sehr eingeschränkt durch die Signaturen abgebildet werden können[2]. Allerdings werden Protokollzustände in den Präprozessoren für die Bearbeitung der Protokolle FTP, HTTP, SMTP und SSH berücksichtigt.

Die Signaturen können entweder aus öffentlichen Quellen oder von der Firma Sourcefire bezogen werden. Die aktuellen Signaturen von Sourcefire sind zwar kostenpflichtig, werden aber nach Ablauf einer zeitlichen Spanne kostenfrei registrierten Benutzern zur Verfügung gestellt.

Zusammenfassung

- Veröffentlichung als Sourcecode unter der GNU General Public Lizenz
- Erkennung und Identifizierung von Angriffen anhand von korrespondierenden Signaturen
- Überwachung des Netzwerkes an zentraler Stelle aus möglich
- Erkennbare Angriffstypen:
  - Alle bekannten Angriffe auf Server und Client-Anwendungen für die Signaturen existieren
  - Portscans
- Nachteile:
  - Keine Erkennung unbekannter Angriffe
  - Keine Überwachung verschlüsselte Verbindungen
  - Hohe Rate an Fehlalarmen typisch

5.2.5 Argos

Argos in [36] ist ein von der freien Universität (Vrije Universiteit) Amsterdam entwickelter Honeypot mit hohem Interaktionsgrad (high interaction honeypot), der insbesondere zur Erkennung von Angriffen auf unbekannte Schwachstellen entwickelt worden. Dabei wird ein generisches Verfahren (*dynamic taint analysis*) eingesetzt, das speziell auf Buffer Overflow und verwandte Schwachstellen abgestimmt ist. Zwar schränkt dies die Klassen von Angriffen ein, jedoch zeigt sich, dass diese Schwachstellen immer noch dominieren. Zudem sind alle wichtigen Komponenten des Betriebssystems und Dienste wie beispielsweise Web-Server von diesen Schwachstellen betroffen gewesen. Dank der generischen Angriffserkennung lassen sich die meisten bekannten Betriebssysteme[3] inklusive Microsoft Windows und Linux als Gast innerhalb von Argos betreiben.

[2] Bro IDS (http://bro-ids.org/) führt aus diesem Grund Abhängigkeitsbedingungen zwischen Signaturen ein.
[3] Da Argos auf Qemu basiert, lassen sich alle Betriebssysteme betreiben, die von Qemu unterstützt werden

Das Prinzip der *dynamic taint analysis* macht sich zu Nutze, dass alle Angriffe auf Buffer Overflow und verwandte Schwachstellen den Kontrollfluss des verwundbaren Programms manipulieren. Dies geschieht, indem Daten an den verwundbaren Dienst oder das Programm gesendet werden, mit denen die Speicherverwaltung nicht zurechtkommt. Typisches Beispiel sind überlange Zeichenketten, die in einen Buffer mit fester Länge kopiert werden. Folge ist, dass der Buffer überläuft und kritische Speicherstrukturen überschreibt. Durch die *dynamic taint analysis* werden alle Daten, die der Computer aus dem Netzwerk empfängt als "verschmutzt" markiert. Alle Daten, die aus der Bearbeitung verschmutzer Daten abgeleitet werden, werden ebenfalls als verschmutzt markiert. Ein Angriff wird erkannt, wenn verschmutzte Daten entweder direkt auf dem Computer ausgeführt werden oder den Kontrollfluss des Programms ändern.

Der entscheidende Vorteil von Argos ist die exakte generische Erkennung von Angriffen. Dadurch können sowohl Fehlalarme (False-Positive) sowie nicht erkannte erfolgreiche Angriffe (False-Negative) weitersgehend ausgeschlossen werden. Da der Angriff erkannt wird, bevor dieser die Kontrolle übernehmen kann, eignet sich Argos auch zum Schutz von Anwendugne und dem Betriebssystem vor der Ausnutzung unbekannten Schwachstellen. Nachteil ist die aufwendige *dynamic taint analysis*, die die Performanz der Programme und Dienste erheblich einschränkt.

Zusammenfassung

- Honeypot mit hohem Interaktionsgrad
- Generische Erkennung von Angriffen auf unbekannte Schwachstellen möglich (keine Angriffssignaturen erforderlich)
- Einsatz zum Schutz kritischer Systeme möglich
- Erkennbare Angriffstypen:
  - Alle Angriffe auf Buffer Overflow und verwandte Schwachstellen werden erkannt, die den Kontrollfluß erfolgreich ändern.
- Nachteile:
  - Honeypot muß angegriffen werden, damit der Angriff erkannt wird
  - Nicht geeignet zum Entdecken Netzwerk-basierter Angriffe (zum Beispiel DDoS)
  - Hohe Anforderungen an Ressourcen

5.2.6 Nepenthes

Ziel von Nepenthes, wie in [4] beschrieben, ist das effektive und automatisierte Sammeln von Malware. Um den hohen Aufwand von Honeypots zu umgehen, werden verwundbare Dienste nur mit einer Zustandsmaschine emuliert. Jeder Angriff auf eine bestimmte Schwachstelle wird durch eine Zustandsmaschine bearbeitet, die innerhalb eines Modules *(Vulnerability Module)* definiert ist. Dafür wird eine Mustersuche mittels regulärer Ausdrücke auf die Netzwerkpakete angewendet. Trifft ein Ausdruck zu, geht die Zustandsmaschine in einen neuen Zustand über. Dabei wird ein feste Antwort an den Angreifer versendet. Beim Erreichen von Endzuständen liegt der Shell-Code des Angriffs vor. Dieser beinhaltet den Code, der durch Ausnutzen der Schwachstelle ausgeführt werden soll. Typischerweise lädt dieser die eigentliche Malware herunter. In Nepenthes wird der Shell-Code zur Auswertung an verschiedene Module (*Shellcode parsing modules*) weitergereicht. Jedes dieser Module ist für einen festen Shellcode entwickelt worden und wendet zur Identifizierung einen regulären Ausdruck an. Trifft dieser zu, werden verschiedenen Merkmale extrahiert. Diese enthalten beispielswseise die URL, von der die Malware heruntergeladen wird. Als Alternative startet Shellcode eine Shell, über die der Angreifer dann beliebige Kommandos auf den kompromittierten System ausführen kann. Dies unterstützt Nepenthes, indem es eine limitierte Shell bereitstellt, durch die Kommandos nur protokolliert aber nicht direkt ausgeführt werden.

Neben dem automatischen Sammeln von Malware kann Nepenthes auch zur Erkennung von Angriffen eingesetzt werden. Anstelle einer Angriffs-Signatur werden die Angriffe durch die Schwachstellen-Module identifiziert. Innerhalb eines Grids kann Nepenthes zur Erkennung von Würmern und automatisierten Scan-und-Exploit Programmen (zum Beispiel Bot-Netzwerken) eingesetzt werden.

Zusammenfassung

- Veröffentlichung als Sourcecode unter der GNU General Public Lizenz
- Honeypot mit mittlerem Interaktionsgrad
- Kommunikation mit Angreifer über vorgefertigte Antworten und Zustandsmaschine
- Fangen von Malware möglich
- Erkennbare Angriffstypen:
  - Bekannte Angriffe, für die ein Schwachstellenmodul existiert
  - Download von Malware
- Nachteile:
  - Nur wenige Angriffe werden erkannt
  - Nicht geeignet zum Entdecken Netzwerk-basierter Angriffe (zum Beispiel DDoS)
  - Honeypot muß angegriffen werden, damit der Angriff erkannt wird
  - Keine Erkennung unbekannter Angriffe
  - Hoher Aufwand für die Erstellung neuer Schwachstellenmodule

5.2.7 OSSEC

OSSEC [35] ist ein Host-basiertes Intrusion Detection System, das Informationen auf dem zu überwachenden System sammelt und analysiert. Dabei werden verschiedenen Aufgaben durchgeführt:

- Auswertung von Log-Dateien des Systems
- Überprüfung der Integrität von Dateien
- Überwachung der Integrität der Windows-Registry
- Erkennung von Anomalien auf dem lokalen System

Die Architektur von OSSEC besteht aus einem zentralen Manager und Agenten, die auf den zu überwachenden Systemen laufen. Der zentrale Manager wertet die Daten als zentrale Instanz aus und speichert die folgenden Datensätze:

- Datenbank der Datei-Prüfsummen
- Die Log-Einträge der überwachten Systeme
- Die Konfiguration
- Der Regelsatz zur Auswertung der Log-Daten

Als Vorteil der Architektur läßt sich ein Netzwerk aus mehreren Systemen überwachen und die Daten werden in einer zentralen Stelle korreliert und auswertertet. Damit lassen sich beispielweise sehr effektiv Angriffe finden, die Passwörter versuchen zu erraten. Allerdings können auch Regeln spezifiziert werden, um Anomalien in den Logs zu finden. Dies kann beispielsweise ein überlanges Request zum Erzeugen eines Buffer Overflows an den Web-Server sein.

Zusammenfassung

- Veröffentlichung als Sourcecode unter der GNU General Public Lizenz
- Host-basiertes IDS
- Auswertung von System-Logs zur Angriffserkennung
- Überprüfen der Integrität von Dateien und Binaries
- Erkennbare Angriffstypen:
  - Bekannte Angriffe, die Spuren in den System-Logs hinterlassen
  - Unbekannte Angriffe, die zu Anomalien in den System-Logs führen oder die Integrität von Dateien oder Binaries verletzen
- Nachteile:
  - Hoher Aufwand, um Policy und Prüfsummen von Dateien zu konfigurieren

5.2.8 Logsurfer

Logsurfer wurde vom DFN-CERT zur Analyse von Log-Einträgen in Echtzeit entworfen. Analog zu OSSEC werden Log-Dateien überwacht, indem eine Policy in Form eines Satzes von Regeln vorgegeben wird. Als Vorteil von Logsurfer können Regeln dynamisch erzeugt und in den Regelsatz integriert werden. Desweiteren können Log-Zeilen in Kontexten aggregiert werden.

Jede Regel besteht unter anderem aus regulären Ausdrucken, die gesuchte Log-Zeilen und Ausschlußkriterien angeben, und einer Aktion. Treffen die Ausdrücke zu, wird die Aktion gestartet. Dies kann das Öffnen eine Kontextes zum Aggregieren von Log-Zeilen, die dynamische Generierung einer neuen Regel oder eine Alarmierung per E-Mail sein. Es existiert eine Erweiterung `Logsurfer+`, die zusätzlich Zähler für Aktionen implementiert. Einsatz sind speziell brute-force Angriffe.

Zusammenfassung

- Veröffentlichung als Sourcecode unter der BSD Lizenz
- Host-basiertes IDS
- Auswertung von System-Logs zur Angriffserkennung
- Sehr mächtige Regeln zur Auswertung der Logs
- Erkennbare Angriffstypen:
  - Bekannte Angriffe, die Spuren in den System-Logs hinterlassen
  - Unbekannte Angriffe, die zu Anomalien in den System-Logs führen
- Nachteile:
  - Hoher Aufwand, um Policy zu konfigurieren

5.2.9 CarmentiS

CarmentiS in [15] erfüllt die Funktionen eines Internet-Frühwarnsystems. Alle Daten werden durch eine Web-Anwendung präsentiert, die als zentrale Informationsdrehscheibe dient. Es werden verschiedenen Benutzergruppen unterschieden:

Analysten werten die Daten in der Frühwarnzentrale aus und erstellen Lagebilder. Ein Lagebild bewertet die aktuelle Bedrohungslage im Internet.

Datenzulieferer betreiben eigene Sensoren, deren Daten an die CarmentiS Datenzentrale gesendet werden.

Kooperierende Einrichtungen CarmentiS unterstützt externe Forscher, die nach Unterzeichnung einer Kooperationsvereinbahrung Zugriff auf anonymisierte Daten erhalten. Weiterhin wird eine Kooperation mit CERTs unterstützt, die die Daten für die Vorfallsbearbeitung verwenden.

Technisch werden verschiedenen Arten von Sensoren betrieben, die jeweils in einer administrativen Domäne stehen. Jede dieser Domänen ist für den Betrieb und die Administration der eigenen Sensoren verantwortlich. Diese Segmentierung des Sensor-Netzwerkes erhöhlt die Flexibilität und Skalierbarkeit der Architektur des Frühwarnsystems.

Die Sensorik umfaßt die Aufzeichnung von Netflows, Netzwerk-basierte IDS und Honeypots, deren Daten in der Frühwarnzentrale gespeichert werden. Die zentrale Speicherung dieser Daten ermöglicht deren Korrelation und Aggregation. Dies ist beispielsweise für brute-force Angriffe hilfreich, bei denen nur die Gesamtheit der Angriffe eine korrekte Interpretierung zuläßt.

Zur Einhaltung des Datenschutzes werden die Daten vor dem Transport in die Frühwarnzentrale pseudonymisiert. Dies ermöglicht dem Datenzulieferer die eigenen Daten ohne Einschränkungen auszuwerten. Für alle anderen ist die Zuordnung der Daten nicht einsichtig. Allerdings läßt sich die Anonymisierung der Daten unter Einverständnis des Datenzulieferers wieder aufheben. Dies kann beispielsweise für die Bearbeitung von Sicherheitsvorfällen notwendig werden.

Zusammenfassung

- Internet-Frühwarnsystem
- Auswertung der Daten in der Frühwarnzentrale
- Unterstützung einer Datenschutzrichtlinie
- Unterstützung unterschiedliche Privilegien und Benutzergruppen
- Erkennbare Angriffstypen:
  - Bekannte Angriffe, die durch Honeypots oder IDS erkannt werden
  - Unbekannte Angriffe, die Anomalien in den Netflows erzeugen
- Nachteile:
  - Keine Unterstützung Host-basierter IDS
  - Konzept des Frühwarnsystems nicht direkt auf das Grid-IDS übertragbar

5.3 Zusammenfassung

Bei den themenverwandten Arbeiten sind viele Ideen und Grundbausteine vorhanden, auf denen das föderierte Grid-IDS aufbauen kann. Keine dieser Arbeiten hat aber eine vollständige Lösung, die alle Anforderungen an das föderierte Grid-IDS berücksichtigt. Schwächen finden sich entweder bei der organisatorischen Einbindung des IDS in das Grid oder dem Datenschutzkonzept.

In vielen der existierenden Produkte werden vereinzelt Anforderungen an ein GIDS umgesetzt. Bislang existiert allerdings noch kein Produkt, welches alle in Kapitel 3.1 erarbeiteten Anforderungen erfüllt. Die meisten eingesetzen Produkte bieten keine gridspezifische Unterstützung und können daher nicht ohne Erweiterungen die durch das Projekt geforderte föderierte Angriffserkennung in einem solch heterogenen Umfeld bieten.

Kapitel 6

Zusammenfassung

Die vorliegende Arbeit hat gezeigt, dass der Bedarf an ein Grid-basiertes Intrusion Detection System gegeben ist. Viele Ressourcenanbieter haben in der Vergangenheit Sicherheitsvorfälle bemerkt, die Grid-Dienste betroffen oder Grid-spezifische Vertrauensbeziehungen der Systeme untereinander ausgenutzt haben. Da das Schadenspotential durch die enorme Rechenleistung und Speichergröße im Grid enorm ist, ist eine zeitnahe Angriffserkennung und -beseitigung essentiell. Ein solches Grid-basiertes Frühwarnsystem gibt es zur Zeit noch nicht und soll durch das Projekt GIDS eingeführt werden.

Die Umgebung, in der das zukünftige Grid-basierte IDS laufen soll, ist hochgradig heterogen. In der vorliegenden Arbeit wurde gezeigt, dass nicht nur die zugrundeliegenden Systeme und die Anforderungen, die die Nutzer des D-Grids haben, sondern auch die möglichen Gefahren und Angriffsszenarien sehr unterschiedlich sind. Gerade bei der Gefahrenminimierung hat sich gezeigt, dass ein einzelnes isoliertes System nicht in der Lage ist, jedes Bedrohungszenario abzudecken. Vielmehr ist es wichtig, dass viele verschiedenartige Systeme miteinander verwoben werden, um kombinierte Angriffe zu erkennen und erfolgreich abzuwehren.

Für die meisten isolierten Angriffsszenarien gibt es bereits gut etablierte Gegenmaßnahmen. In dieser Arbeit wurde jedoch herausgestellt, dass es bisher noch keine zufriedenstellenden Mechanismen oder Methoden gibt, um diese meist isolierten Einzelsysteme miteinander zu kombinieren und dabei die Besonderheiten des D-Grid zu wahren. Diese Lücke soll durch das Projekt GIDS gefüllt werden, so dass es am Ende dem Anspruch eines „föderierten“ Intrusion Detection Systems gerecht wird. Ein Ergebnis des vorliegenden Dokuments ist unter anderem ein Katalog mit Kriterien für die Auswahl und Bewertung von Intrusion Detection Systemen für ihre Eignung zum Einsatz innerhalb eines Grids. Eine zusammenfassende Übersicht des Katalogs ist in Kapitel 3.3 in Tabelle 3.20 auf Seite 42 zu finden.

Bis das Projekt GIDS allen Anforderungen, die in Kapitel 3 erhoben wurden, genügt, werden noch viele Vorarbeiten nötig sein. Gerade die Wahrung des Datenschutzes und die Definition des Austauschformats sind zwei sehr essentiell wichtige Punkte. Zum einem ist eine Kooperation mit den Ressourcenanbietern eine der Grundvoraussetzungen für das Gelingen des Projektes. Diese werden jedoch fordern, dass man für die Nutzung der anfallenden Daten die organisatorischen Policies und gesetzlichen Vorschriften beachtet. Zum anderen sind viele Eigenentwicklungen in der D-Grid-Landschaft zu finden. Da man davon ausgehen kann, dass diese keine einheitlichen Schnittstellen und Logging-Formate haben, muss vor einer kooperativen Nutzung der Daten eine Harmonisierung stattfinden.

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

[1] *http://www.carmentis.org/.*

[2] Nepenthes - finest collection. *http://nepenthes.carnivore.it/.*

[3] Technical report, October 2007.

[4] Paul Baecher, Markus Koetter, Maximillian Dornseif, and Felix Freiling. The nepenthes platform: An efficient approach to collect malware. In *In Proceedings of the 9 th International Symposium on Recent Advances in Intrusion Detection (RAID*, pages 165–184. Springer, 2006.

[5] Bernd Bruegge and Allen H. Dutoit. *Object-Oriented Software Engineering: Using UML, Patterns and Java, Second Edition.* Prentice Hall, 2003.

[6] Andreas Bunten. Neues aus dem DFN-CERT. 49. DFN Betriebstagung, Berlin *http://www.dfn.de/fileadmin/3Beratung/Betriebstagungen/bt49/forum-sicherheit2-bunten.pdf*, 2008.

[7] Ong Tian Choon and Azman Samsudin. Grid-based Intrusion Detection System. In *Proceedings of the 9th Asia-Pacific Conference on Communications (APCC)*, volume 3, pages 1028–1032, September 2003.

[8] January 2007.

[9] Claudia Eckert. *IT-Sicherheit Konzepte-Verfahren-Protokolle.* Oldenburg Wissenschaftsverlag GmbH, 2008.

[10] Guofu Feng, Xiaoshe Dong, Weizhe Liu, Ying Chu, and Junyang Li. GHIDS: Defending Computational Grids against Misusing of Shared Resources. In *Proceedings of the IEEE Asia-Pacific Conference on Services Computing (APSCC)*, pages 526–533, 2006.

[11] European Policy Management Authority for Grid Authentication. *http://www.eugridpma.org/.*

[12] Ian Foster. What is the grid? A three point checklist. *GRIDtoday*, 1(6), July 2002.

[13] OWASP Foundation. OWASP TESTING GUIDE. *http://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf*, 2008.

[14] Xun Gong, Tao Li, Tiefang Wang, Jin Yang, Gang Liang, and Xiaoqin Hu. Grid intrusion detection based on immune agent. In *ICNC (2)*, pages 73–82, 2006.

[15] Bernd Grobauer, Jens Ingo Mehlau, and Jürgen Sander. Carmentis: A co-operative approach towards situation awareness and early warning for the internet. In *IMF Conference Proceedings*, pages 55–66, 2006.

[16] Hegering, Hiller, Maschuw, Reinefeld, and Resch. D-Grid: Auf dem Weg zur eScience in Deutschland. (Strategiepapier), 2003.

[17] Rolf Hennicker. Objektorientierte Software-Entwicklung, 2006.

[18] R. Housley, W. Ford, W. Polk, and D. Solo. Internet X.509 Public Key Infrastructure Certificate and CRL Profile. RFC 2459 (Proposed Standard), January 1999. Obsoleted by RFC 3280.

[19] J. Howard and T. Longstaff. A Common Language for Computer Security Incidents. Technical Report, Sandia National Labaratories *www.cert.org/research/taxonomy_988667.pdf*, 1998.

[20] K. Hwang, Y. Kwok, S. Song, M. Cai, R. Zhou, Y. Chen, Y. Chen, and X. Lou. Gridsec: Trusted grid computing with security binding and self-defense against network worms and ddos attacks. In *International Workshop on Grid Computing Security and Resource Management (GSRM'05),in conjunction with ICCS 2005*, May 2005.

[21] IETF. Public key infrastructure - certificate and certificate revocation list (crl) profile. *http://tools.ietf.org/html/rfc5280*.

[22] IETF. Public key infrastructure - online certificate status protocol. *http://tools.ietf.org/html/rfc2560*.

[23] IETF. Public key infrastructure (pki) - proxy certificate profile. *http://www.ietf.org/rfc/rfc3820.txt*.

[24] S. Jha, O. Sheyner, and J. Wing. Two formal analys s of attack graphs. In *CSFW '02: Proceedings of the 15th IEEE workshop on Computer Security Foundations*, page 49, Washington, DC, USA, 2002. IEEE Computer Society.

[25] Stuart Kenny and Brian Coghlan. Grid-wide intrusion detection, December 2004.

[26] Stuart Kenny and Brian Coghlan. Towards a grid-wide intrusion detection system. In *Proceedings of the EGC : European grid conference*, pages 275–284, February 2005.

[27] Jan Kohlrausch. Angriffe auf Webserver durch PHP Input Wrapper. DFN-CERT Sicherheitsbulletins *http://www.dfn-cert.de/informationen/Sicherheitsbulletins/dsb-2009-01.html*, 2009.

[28] Jake Kouns, Brian Martin, David Shettler, and Kelly Todd. DATALOSTdb, Open security foundation. *http://datalossdb.org*, 2009.

[29] Lancope. StealthWatch Produktinformationen. *http://www.lancope.com/downloads/StealthWatch System Family Brochure.pdf*, 2009.

[30] Fang-Yie Leu, Ming-Chang Li, Jia-Chun Lin, and Fu-Yi Yang. Integrating Grid with Intrusion Detection. In *Proceedings of the 19th IEEE International Conference on Advanced Information Networking and Applications (AINA)*, pages 304–309, March 2005.

[31] Fang-Yie Leu, Jia-Chun Lin, Ming-Chang Li, and Chao-Tung Yang. A Performance-Based Grid Intrusion Detection System. In *Proceedings of the 29th International Computer Software and Applications Conference (COMPSAC)*, volume 1, pages 525–530, July 2005.

[32] MediGRID. *http://www.medigrid.de*.

[33] Milw0rm Exploit Archive. *http://www.milw0rm.com/*.

[34] Jiancheng Ni, Zhishu Li, Jirong Sun, and Jianchuan Xing. Self-adaptive Intrusion Detection System for Computational Grid. In *Proceedings of the 1st IEEE & IFIP International Symposium on Theoretical Aspects of Software Engineering (TASE)*, pages 97–106, June 2007.

[35] OSSEC Homepage. *http://www.ossec.net/*, 2009.

[36] G. Portokalidis, A. Slowinska, and E. Markatos. Argos: an emulator for fingerprinting zero-day attacks. In *Proceedings of ACM SIGOPS Eurosys 2006*, April 2006.

[37] Marsh Ray and Steve Dispensa. Renegotiating TLS. *http://extendedsubset.com/?p=8*, 2009.

[38] James Robertson and Suzanne Robertson. Volere requirements specification template, August 2007.

[39] Alexandre Schulter, Julio Albuquerque Reis, Fernando Koch, and Carlos Becker Westphall. A Grid-based Intrusion Detection System. In *Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL)*, April 2006.

[40] Alexandre Schulter, Fabio Navarro, Fernando Koch, and Carlos Becker Westphall. Towards Grid-based Intrusion Detection. In *Proceedings of the 10th Network Operations and Management Symposium (NOMS)*, pages 1–4, April 2006.

[41] Ulrich Schwardmann. Gefahrenabwehr bei einem local root exploit. *http://www.d-grid.de/uploads/media/Schwardmann-Gefahrenabwehr_bei_einem_local_root_exploit.pdf*, 2009.

[42] P.F. Silva, C.B. Westphall, C.M. Westphall, and M.D. de Assuncao. Design and evaluation of a grid computing based architecture for integrating heterogeneous idss. In *Proceedings of the Global Telecommunications Conference (GLOBECOM)*, pages 338–342, November 2007.

[43] Snort Homepage. *http://www.snort.org/*, 2009.

[44] Marc Stevens. Chosen-prefix collisions for md5 and applications. *Journal of Cryptology*, 2009.

[45] Symantec. Symantec Global Internet Security Threat Report. *http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_-security_threat_report_xiii_04-2008.en-us.pdf*, 2008.

[46] Kevin Timm. IDS Evasion Techniques and Tactics. *http://www.securityfocus.com/infocus/1577*, 2002.

[47] Mohamed F. Tolba, Mohammad S. Abdel-Wahab, Ismail A. Taha, and A. M. Al-Shishtawy. Distributed Intrusion Detection System for Computational Grids. In *Proceedings of the 2nd International Conference on Intelligent Computing and Information Systems*, March 2005.

[48] Mohamed F. Tolba, Mohammad S. Abdel-Wahab, Ismail A. Taha, and A. M. Al-Shishtawy. GIDA: Toward Enabling Grid Intrusion Detection Systems. In *Proceedings of the 5th IEEE International Symposium on Cluster Computing and the Grid*, May 2005.

[49] Andreas Bunten und Alex Everett. Advisory: Linux Compromises. *http://its.unc.edu/ccm/groups/public/@its/@security/documents/content/ccm3_-008080.pdf*, 2008.

[50] US-CERT. Current Activity: SSH Key-based Attacks, 2008.

[51] Torsten Voss. Neues aus dem DFN-CERT. 50. DFN Betriebstagung, Berlin *http://www.dfn.de/fileadmin/3Beratung/Betriebstagungen/bt50/forum-sicherheit-Neuescert_tv.pdf*, 2009.

[52] Guiling Zhang and Jizhou Sun. Grid intrusion detection based on soft computing by modeling real-user's normal behaviors. In *Proceedings of the Granular Computing (GrC) – IEEE International Conference*, pages 558–561, May 2006.