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

Grobskizze einer Architektur für ein Grid-basiertes IDS (MS 10)
Meilenstein zum Abschluss des Arbeitspakets 5.1

Autoren:
Dr. Wolfgang Hommel (Leibniz-Rechenzentrum)
Dr. Nils gentschen Felde (Ludwig-Maximilians-Universität München)
Felix von Eye (Leibniz-Rechenzentrum)
Jan Kohlrausch (DFN-CERT GmbH)
Christian Szongott (Regionales Rechenzentrum für Niedersachsen)

GEFÖRDERT VOM

Inhaltsverzeichnis

Kapitel 1

Einleitung

Dieses Dokument präsentiert als Ergebnis des Arbeitspakets 5.1 des Projekts „Ein Grid-basiertes, föderiertes Intrusion Detection System zur Sicherung der D-Grid Infrastruktur“ (GIDS) eine Grobarchitektur für ein 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

Im bisherigen Projektverlauf wurde bereits ein Anforderungs- und Kriterienkatalog erstellt, der im Meilensteindokument [7] in den Kapiteln 3 und 4 zu finden ist. Vor diesem Hintergrund skizziert Kapitel 2 einen neuartigen Ansatz für ein Intrusion Detection System für Grids. Dabei wird die grundlegende Idee der kooperativen Nutzung von lokalen Sicherheitssystemen und der Austausch von Angriffsdaten verfolgt.

Im darauffolgenden Kapitel 3 werden die Anforderungen an GIDS konkretisiert und erste Rollen und Komponenten spezifiziert. Die nötigen Komponenten werden aufgrund von gegebenen Anforderungen spezifiziert.

Nachgelagert an den Architekturentwurf gibt Kapitel 4 einen Ausblick auf die nächsten beiden Meilensteindokumente, die das *Informationsmodell und Datenaustauschformat* (MS 12) und das *Datenschutzkonzept* (MS 13) zum Thema haben. Ebenfalls werden in diesem Kapitel Abhängigkeiten zwischen dem Datenschutzkonzept und dem Informationsmodell bzw. Datenschutzformat einerseits und dem Architekturentwurf von GIDS andererseits thematisiert.

Abschließend stellt Kapitel 5 einige konzeptionelle Implementierungsmöglichkeiten für den Datenaustausch vor und bewertet ihre Eignung für GIDS.

Kapitel 2

Idee zum Aufbau eines Grid-basierten IDS

Bereits einleitend in [7] ist die Idee aufgekommen, GIDS als Föderation aus bestehenden, für die Ressourcenanbieter eines Grids spezifischen, sicherheitsrelevanten Komponenten hin zu einem Grid-weiten Frühwarnsystem zu konzipieren. Aus der Analyse in Kapitel 3 der genannten Arbeit sind unter anderem Anforderungen abgeleitet worden, die die Autonomie der einzelnen Teilnehmer eines Grid-basierten IDS fordern, was nicht zuletzt für die Akzeptanz eines solchen Systems zwingend notwendig ist. Daraus abgeleitet bedingt sich eine verteilte Struktur und es entsteht eine lose Kopplung der am GIDS beteiligten Partner, die daraus folgend jeder für sich organisatorisch und administrativ wie auch technisch unabhängig und autonom agieren können und in vielen Bereichen sogar müssen.

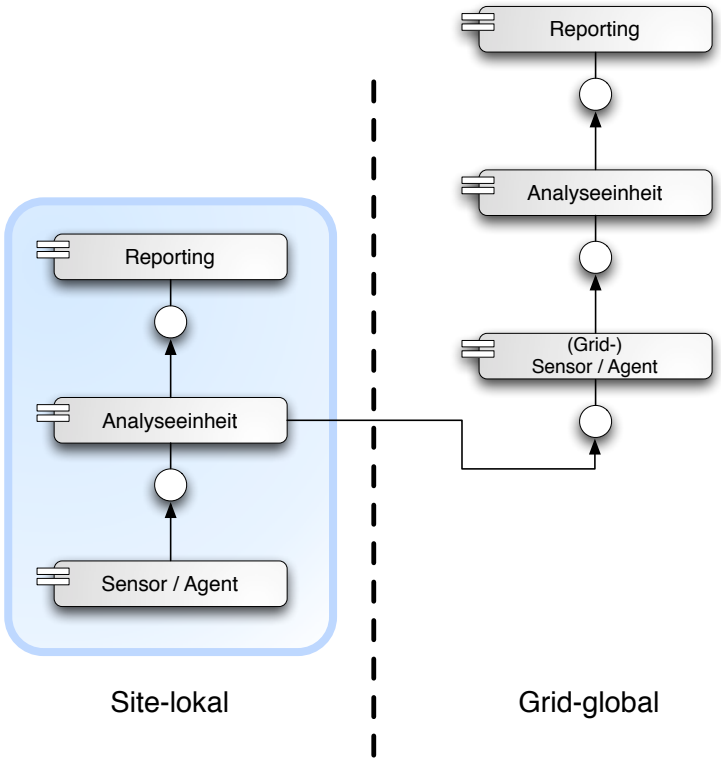


Abbildung 2.1: Grundlegende Idee zum Aufbau eines Grid-basierten IDS

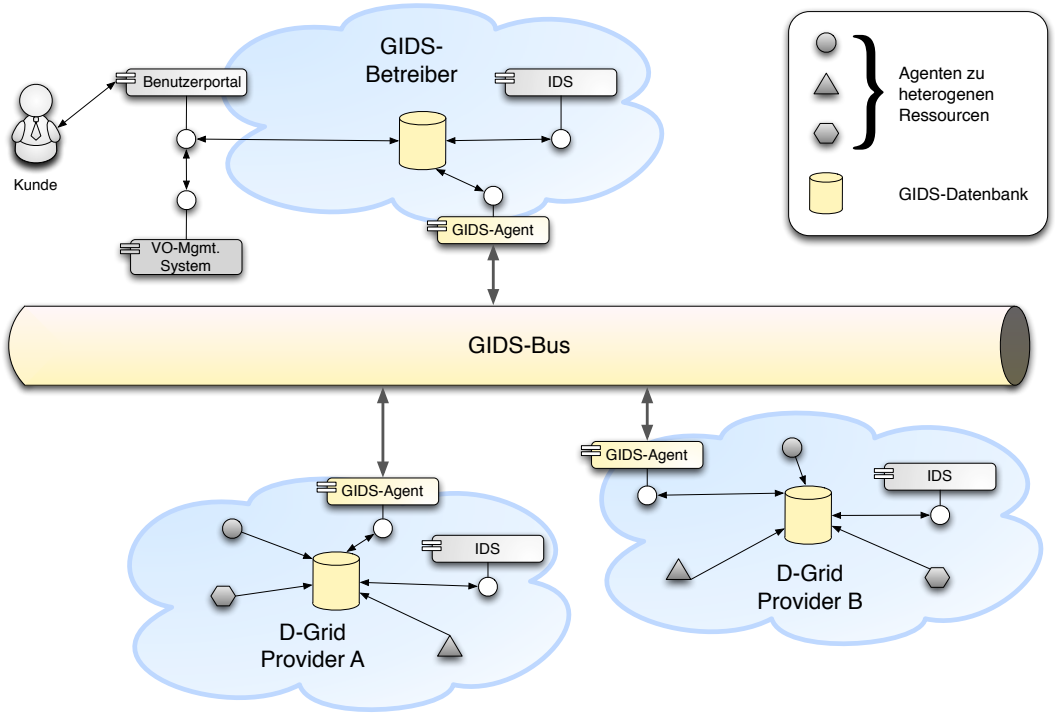


Abbildung 2.2: Grobgranulare Übersicht der Architektur des GIDS

Für den hiesigen Anwendungsfall zur Konzeption eines föderierten Frühwarnsystems unter Wahrung der Autonomie aller teilnehmenden Partner bietet sich folglich eine Art der Schachtelung dieses allgemeingültigen Aufbaus an, wie sie in Abbildung 2.1 illustriert ist. Ein Informationslieferant für das Grid-basierte IDS, also ein Grid-Sensor oder -Agent, soll durch eine administrative Domäne beziehungsweise einen Ressourcenanbieter im Grid (hier auch synonym als Site bezeichnet) gegeben sein. Durch eine solche Konzeption lassen sich prinzipiell sowohl sämtliche Rohdaten (zum Beispiel von bestehender, Site-spezifischer IDS-Sensorik, Firewall-Logdateien, Netflow-Traces etc.) als auch veredelte Informationen durch beispielsweise bestehende, Site-lokale IDS-Installation in das Grid-basierte Frühwarnsystem einbringen.

Diese grundsätzliche Idee führt nun weiter zu einem Grid-globalen Aufbau eines IDS wie es in Abbildung 2.2 wenig detailliert aus einer Vogelperspektive dargestellt ist. Jeder Teilnehmer des GIDS erhält eine zentrale Datenbank, in die alle verfügbaren, für die Sicherheit relevanten Informationen abgelegt werden können. Wie bereits zuvor angesprochen können dies zum einen Rohdaten (z.B. von versuchten Zugriffen auf gesperrte Ports an einer Firewall) oder auch bereits veredelte oder aggregierte Informationen wie Berichte lokal installierter IDS sein. In jedem Fall gilt es zu beachten, dass an dieser Stelle eine Einigung auf ein einheitliches Daten- und Informationsmodell notwendig ist. Eine Detaillierung wird später durchgeführt. An einen solchen zentralen Datenspeicher angeschlossen kann ein Agent unter Beachtung einiger notwendiger Randbedingungen Informationen an ein Grid-weites IDS weiterreichen.

Weiter kann dieser Agent Informationen aus dem GIDS entgegennehmen und im zentralen Datenspeicher hinterlegen. Zur Kommunikation bietet sich ein Multicast oder sogar Broadcast der Daten zwischen den Agenten an, da dadurch bedingt ein verteilter Ansatz mit einer vollständigen Datenreplikation verwirklicht werden kann. Schlussendlich hat jeder teilnehmende Ressourcenanbieter die Möglichkeit, eine eigene Instanz des GIDS auf Basis seiner lokal vorgehaltenen Daten zu betreiben.

Aus der Anforderungsanalyse ist hervorgegangen, dass ein Betreiber für eine Grid-globale Instanz des GIDS, zusätzlich zu den Site-lokal betriebenen Instanzen, notwendig ist, um einen kunden- und VO-orientierten Dienst schaffen und im Grid bereitstellen zu können. Dieser

Betreiber unterscheidet sich von den Ressourcenanbietern im Wesentlichen dadurch, dass er keine eigene Sensorik bestehender Systeme mit einbringen kann, da er in seiner Rolle nicht als Ressourcenanbieter fungiert. Zudem impliziert er keinen zentralisierten Aufbau des GIDS, wie auch aus den folgenden Teilabschnitten hervorgeht. Eine Detaillierung des Aufbaus eines Grid-basierten Frühwarnsystems sowohl auf Seiten eines Ressourcenanbieters als auch auf Seiten des Betreibers des GIDS findet sich in den folgenden Kapiteln.

Kapitel 3

Architekturentwurf

Im Rahmen eines Software-Entwurfprozesses werden aus einer fundierten Anforderungsanalyse und den daraus abgeleiteten Anforderungen an ein zu entwickelndes System, wie in [7] durchgeführt, Entwurfskriterien und eine Architektur strukturiert hergeleitet. In diesem Kapitel fasst Abschnitt 3.1 nochmal die in [7] Anforderungen in einer geordneten Weise zusammen, bevor ein erster grober Architekturentwurf für ein IDS im D-Grid vorgestellt wird. Die Abschnitte 3.2 und 3.3 erörtern nachfolgend weitere im Rahmen von GIDS notwendige Rollen bzw. verwendbare Entwurfsmuster, die eine potentielle Anwendung in einem nachgelagerten Implementierungsschritt finden könnten.

3.1 Strukturierte Ableitung eines Architekturentwurfs

In [7] in Kapitel 3.3 und ergänzend in 4.6 wurden eine Reihe von Kriterien für ein Grid-IDS angeführt. Diese wurden in fünf Kategorien eingeteilt. Der Übersicht halber werden im Folgenden alle Anforderungen geordnet nach den Kategorien noch einmal wiederholt.

Funktionale Anforderungen:

- **F01:** Unterstützung verschiedener Granularitätsstufen bei der Berichterstattung
- **F02:** Berichterstattung zu qualitativ differierenden Angriffen
- **F03:** Aussagekräftige Informationsaufbereitung
- **F04:** Zugriffsmöglichkeit auf Sensordaten
- **F05:** Variationsmöglichkeit der Informationsquellen/Datenbasis zur Laufzeit
- **F06:** Proaktive Benachrichtigung der Kunden
- **F07:** Nutzung verschiedener Kommunikationsmodelle (Push, Pull, Stream)
- **F08:** Aggregatbildung
- **F09:** Informationspräsentation im Grid-Portal
- **F10:** Nutzung bestehender Grid-Dienste
- **F11:** Anbindung an bzw. Nutzung von bestehenden VO-Managementsystemen
- **F12:** Aussagekräftige Informationsaufbereitung

Nichtfunktionale Anforderungen:

- **N01:** Integrierbarkeit in bestehende Management-Werkzeuge
- **N02:** Interoperabilität
- **N03:** Mandantenfähigkeit
- **N04:** Nachvollziehbarkeit durchgeführter Anfragen
- **N05:** Portabilität

N06: Wiederverwendbarkeit

N07: Dezentrale Organisation

N08: Einheitliche Schnittstellen

N09: Erweiterbarkeit und Flexibilität

N10: Hohe Leistungsfähigkeit

N11: Skalierbarkeit

N12: Dynamik der Nutzer und VOs

N13: Dynamik der Ressourcen

N14: Unterstützung etablierter (Grid-) Standards

N15: Unterstützung Virtueller Organisationen

N16: Interoperabilität der Sensoren

Sicherheitsanforderungen:

Kryptographische Anforderungen:

S01: Vertraulichkeit von Daten und Nachrichten

S02: Authentizität von Daten und Nachrichten

S03: Integrität von Daten und Nachrichten

S04: Einsatz symmetrischer und/oder asymmetrischer Kryptografie

S05: Kanal- oder nachrichtenbasierte Kommunikationssicherung

S06: Schutz der Grid-IDS Daten

Nutzerverwaltung:

S07: Integration in PKI

S08: Delegation von Identitäts- und Berechtigungsnachweisen

S09: Single Sign-On mit Proxy-Zertifikaten

S10: Einbindung bestehender AA-Mechanismen

S11: Zugriffsbeschränkung auf Informationen

Organisatorische und Datenschutzanforderungen:

Organisatorische Anforderungen:

D01: Etablierung einer vertrauenswürdigen Koordinationseinheit

D02: Prozessspezifikation für (Signatur-) Updates

D03: Gewährleistung der Autonomie beteiligter Informationsanbieter

D04: Weitergehende Kooperation

D05: Juristisch verwertbare Speicherung der Daten

Datenschutz:

D06: Anonymisierungs- und/oder Pseudonymisierungsmöglichkeiten

D07: Durchsetzung des Datenschutzes

D08: Nachhalten historischer Berichte

D09: Archivierung von Sensordaten

Anforderungen an die Erkennungsleistung:

Örtliche Aspekte:

E01: Schutz der potentiellen Angriffsziele

E02: Geeignete Sensorplatzierung

E03: Diversität

Angriffstypen und -muster:

E04: Erkennung verschiedener Angriffstypen (aktiv, passiv/autonom, DoS)

E05: Entdecken kurzzeitig angelegter bis hin zu zeitlich lang andauernder Angriffe

Im Folgenden beschreibt dieser Abschnitt einzelne, organisatorisch unabhängige Architekturteile, die in ihrer Summe das Grobkonzept des Grid-basierten IDS bilden. Die einzelnen dafür notwendigen Komponenten lassen sich aus den oben genannten erhobenen Anforderungen an ein GIDS ableiten, was nachfolgend in umgekehrter Reihenfolge anhand der fünf Anforderungskategorien kurz erörtert wird. Eine detaillierte Beschreibung der einzelnen Komponenten und deren Zusammenspiel ist dann in den Unterabschnitten dieses Kapitels zu finden.

Erkennungsleistung. Die Zweiteilung der Anforderungen zur Erkennungsleistung kann sich in ebenfalls zwei Komponenten des Systems widerspiegeln. Örtliche Aspekte können dabei durch die Einführung von *Agent*en, die verschiedene Informationsquellen (Firewalls und ihre Log-Dateien, lokale IDS-Instanzen etc.) anbinden, befriedigt werden. Die Erkennung verschiedener Angriffsmuster und -typen fordert die Notwendigkeit nach austauschbaren Analysefunktionen in einer *lokalen (G)IDS-Instanz* mit angeschlossener *GIDS-Datenbank*, um auch zeitlich lang andauernde Angriffe geeignet erkennen zu können.

Organisatorische und Datenschutzanforderungen. Zur (technischen) Durchsetzung von Informationsverbreitungsrichtlinien und der Gewährleistung von Datenschutzrichtlinien am GIDS partizipierender Ressourcenanbieter wird zum einen ein *Filter* und zum anderen ein *Anonymisierer/Pseudonymisierer* notwendig. Weiterhin erfordert die Anforderung „Weitergehende Kooperation“ eine Möglichkeit, Angriffe, für deren Entdeckung Sensoren ungeeignet sind, zu melden. Dafür bietet es sich an, einen Betreiber des GIDS einzuführen, der die notwendigen Schnittstellen bereit hält.

Sicherheitsanforderungen. Zur Realisierung kryptographischer Anforderungen bei der Interkommunikation der beteiligten Parteien bedarf es eines *GIDS-Agent*en, während die Anforderungen an eine Nutzerverwaltung und entsprechende AA-Mechanismen eine Anbindung an die bestehenden VO-Managementsysteme notwendig machen.

Nichtfunktionale Anforderungen. Aus dem umfangreichen Bereich der nichtfunktionalen Anforderungen lassen sich eine Menge Komponenten und Schnittstellen ableiten. Insbesondere folgt aus den Grid-bedingten Anforderungen ein weiteres Mal die Anbindung des GIDS an die bestehenden VO-Managementsysteme sowie auch an Monitoring-Komponenten bzw. deren Teilfunktionalität der bijektiven Abbildung von VOs zu den von ihnen im Grid genutzten Ressourcen. Durch Anforderungen wie Wiederverwendbarkeit, Erweiterbarkeit oder auch Flexibilität lässt sich einmal mehr die bereits zuvor erwähnte Komponente des *Agent*en ableiten. Zusätzlich bedingt die Forderung nach einer großen Leistungsfähigkeit und Skalierbarkeit auch die Möglichkeit der Informationsverdichtung. Daraus folgt direkt die Notwendigkeit einer *Aggregator/Verdichter*-Komponente. Weiterhin motivieren die nichtfunktionalen Anforderungen ein einheitliches Datenaustauschformat.

Funktionale Anforderungen. Insbesondere die Einführung eines Kundenbegriffs im Rahmen Grid-basierter IDS motiviert die Existenz eines Betreibers des GIDS sowie die dazu gehörigen Komponenten. Natürlich muss auch mindestens eine *globale GIDS-Instanz* mit dazugehöriger *GIDS-Datenbank* und einem *GIDS-Agent*en zur Kommunikation gegeben sein. Zusätzlich bedarf es jedoch eines *Benutzerportal*s und einer Komponente für eine *proaktive Benachrichtigung* und deren Anbindung an VO-Managementsysteme sowie die Notwendigkeit der Abbildung von VOs zu den von ihnen genutzten Ressourcen.

Im weiteren Verlauf dieses Kapitels wird auf die genaue Funktionalität der geforderten Komponenten und deren Zusammenspiel sowie auf erste Hinweise auf eine mögliche technische Umsetzung eingegangen. Abschnitt 3.1.1 geht genauer auf die Architektur auf Seiten eines Ressourcenanbieters ein und Abschnitt 3.1.2 stellt den Aufbau auf Seiten des Betreibers des GIDS

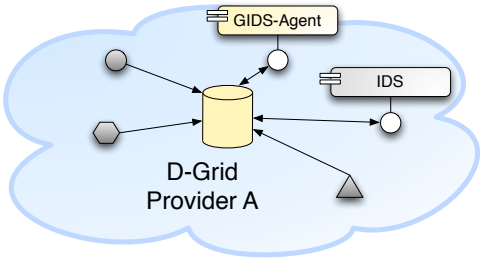


Abbildung 3.1: Architekturüberblick auf Seiten einer teilnehmenden Domäne

dar. Abschließend wird die Möglichkeit der Erweiterung des Gesamtsystems um zusätzliche Informationsanbieter in Abschnitt 3.2.1 kurz erläutert.

3.1.1 Architektur auf Seiten eines Ressourcenanbieters

Eine grobe Übersicht über den Aufbau des Systems innerhalb der administrativen Grenzen eines Ressourcenanbieters ist in Abbildung 3.1 dargestellt.

Die nachfolgend verwendeten Komponenten zum Aufbau des GIDS auf Seiten eines Ressourcenanbieters lassen sich vor allem aus dem oben zusammengefassten Kriterienkatalog für IDS im Grid-Umfeld ableiten. So wird der Forderung nach der Möglichkeit der Aggregatbildung auch aus Gründen der Performanz, der Beachtung von Datenschutzaspekten (inkl. der Archivierung von Sensordaten und Berichten) und der Durchsetzung von Informationsverbreitungsrichtlinien jeweils durch die nachfolgend beschriebenen Komponenten der Datenbank, des Filters, des Aggregators bzw. Verdichters sowie des Anonymisierers und Pseudonymisierers Rechnung getragen. Die Art und Weise des Zusammenspiels dieser Komponenten resultiert insbesondere aus Grid-bedingten Anforderungen wie z.B. Dynamikaspekten und Gesichtpunkten der Leistungsfähigkeit und Performanz, während geeignete Implementierungstechniken weitere Anforderungen, wie zum Beispiel kryptographische oder die Erkennungsleistung des IDS betreffende Anforderungen, befriedigen können.

Um für ein Grid-weites IDS eine vollständige Datenreplikation gewährleisten zu können, kommt bei jedem Ressourcenanbieter eine zentrale Datenbank zum Einsatz. Diese Datenbank wird primär aus drei verschiedenen Informationsquellen gespeist:

Agent. Bei jedem Ressourcenanbieter können mehrere Agenten in verschiedenen Ausprägungen installiert sein und betrieben werden. Agenten dienen dazu, dass Informationen bestehender Sicherheitsvorkehrungen (z.B. Netflow Traces oder Firewall Logs) im zentralen Datenspeicher abgelegt werden können.

GIDS-Agent. In Abgrenzung zu den Agenten ist der GIDS-Agent für die Kommunikation mit den anderen Teilnehmern des GIDS verantwortlich. Zum einen verschickt er ausgewählte Informationen (siehe hierzu die Vorverarbeitungsschritte weiter unten) an andere am GIDS teilnehmende GIDS-Agenten, zum anderen empfängt er eben solche Daten von anderen GIDS-Agenten und hinterlegt sie ebenfalls in der zentralen Datenbank.

Lokale (G)IDS-Instanz. Dadurch, dass ein (lokaler) Datenbestand sämtlicher im GIDS „öffentlich“ verfügbarer Informationen vorliegt, besteht die Möglichkeit, bei jedem Ressourcenanbieter eine eigene Instanz des GIDS zu betreiben. Dadurch bedingt, dass der Site-spezifische Datenbestand unter anderem auch nicht im GIDS veröffentlichte Informationen enthalten kann, eignet sich diese Instanz des GIDS ebenfalls als mögliche Instanz eines lokalen, Site-spezifischen IDS. Berichte dieses (G)IDS werden ebenfalls in der lokalen Datenbank abgelegt.

Bevor es zur Veröffentlichung jedweder Information im Grid durch den GIDS-Agenten kommt, durchlaufen sämtliche Informationen noch drei Vorverarbeitungsschritte.

Filter. Neue Datensätze, die in die zentrale Datenbank geschrieben werden, werden an einen Filter weitergereicht. Die primäre Aufgabe des Filters ist nun das Durchsetzen der Site-spezifischen Informationsverbreitungsrichtlinien. In Abgrenzung zu Datenschutzbestimmungen sind Informationsverbreitungsrichtlinien zumeist Bestandteil lokaler Sicherheitsrichtlinien, die zum Beispiel die Vermeidung der Verbreitung interner Topologiemerkmale, Sicherheitsverletzungen etc. fordern. Der Filter kann einen eingehenden Datensatz auf Grund bestimmter Auswahlkriterien verwerfen oder auch passieren lassen.

Eine weitere wichtige Aufgabe des Filters ist es, Datensätze, die von einem GIDS-Agenten in die Datenbank geschrieben wurden, auszufiltern. Sollte dies nicht passieren, so kann es zu Duplikaten in den Datenbeständen und somit zwangsläufig zu Endlosschleifen der Nachrichten kommen, wodurch in kürzester Zeit eine Überlastsituation (Netzkapazitäten, Speicherkapazität der Datenbanken, Informationsflut für analysierenden IDS-Instanzen etc.) im GIDS zustande kommen würde.

Aggregator/Verdichter. Diejenigen Datensätze, die nicht zuvor durch den Filter aus dem Informationsstrom entfernt worden sind, können in dieser Komponente aggregiert oder verdichtet werden. Eine Aggregation (auch Konsolidierung oder Verdichtung) bezeichnet das Zusammenfassen vieler Daten mit wenig Informationen zu wenigen Daten mit entsprechend hohem Informationsgehalt. Für eine Aggregation wird eine Aggregationsfunktionen benötigt, die zum Beispiel im Falle einer Menge von Zahlen der Mittelwert, das Minimum, das Maximum oder die Summe sein können. Durch den Schritt der Aggregation kann also eine Datenverdichtung erfolgen und somit das Aufkommen an Informationen nochmals deutlich gesenkt werden.

Anonymisierer/Pseudonymisierer. Bevor die (aggregierten) Datensätze die administrativen Grenzen eines GIDS-Teilnehmers verlassen, müssen neben den Informationsverbreitungsrichtlinien, die durch die Filterkomponente gewahrt worden sind, auch Datenschutzbestimmungen eingehalten werden. Insbesondere rechtliche Randbedingungen zwingen einen Ressourcenanbieter unter anderem dazu, keine personenbezogenen Daten nach außen zu tragen, was durch den Vorgang der Anonymisierung oder einer Pseudonymisierung gewährleistet wird.

Die Reihenfolge, in der alle Informationen aus der Datenbank die drei zuvorstehenden Komponenten durchlaufen, ist prinzipiell für die Funktionalität nicht entscheidend. Bei der Anordnung dieser Komponenten wird wohl aus Effizienzgründen an erster Stelle eine Filterung (also Löschung „unerwünschter“ Datensätze), dann eine Informationsverdichtung (also eine nochmalige Datenreduktion) und erst abschließend eine Anonymisierung bzw. Pseudonymisierung vorgenommen.

3.1.2 Architektur auf Seiten des Betreibers des GIDS

Die Architektur auf Seiten des Betreibers des GIDS steht in Anlehnung an den Aufbau des Systems auf Seiten eines Ressourcenanbieters. In Abgrenzung zu einem Ressourcenanbieter stellt der Betreiber des GIDS in der Regel jedoch keine Rohdaten für eine gemeinschaftliche Angriffserkennung zur Verfügung, da er nicht über entsprechende Datenquellen verfügt. Vielmehr stellt er einen Grid-Dienst zur Verfügung, der eine Berichterstattung und Darstellung der im GIDS verfügbaren Informationen und Berichte für die unterschiedlichen Nutzergruppen (Ressourcenanbieter, VOs etc.) anbietet. Entsprechend ist die Architektur auf Seiten des Betreibers des GIDS um die Komponenten zur Datenakquise (die Agenten) und die Komponenten zur datenschutzkonformen Informationsaufarbeitung bereinigt. Zur Dienstbereitstellung jedoch werden Anbindungen an Grid-typische Dienste (z.B. VO-Managementsysteme) und eine Erweiterung um ein dem Grid konformes Dienstportal vorgenommen. Abbildung 3.2 stellt den groben Aufbau des GIDS auf Seiten seines Betreibers graphisch dar.

GIDS-Agent und Datenspeicher. Sowohl aus Architektur- als auch aus Implementierungssicht ist der GIDS-Agent und der Datenspeicher identisch mit den vergleichbaren Komponenten auf Seiten eines Ressourcenanbieters. Im Falle des Betreibers des GIDS ist es

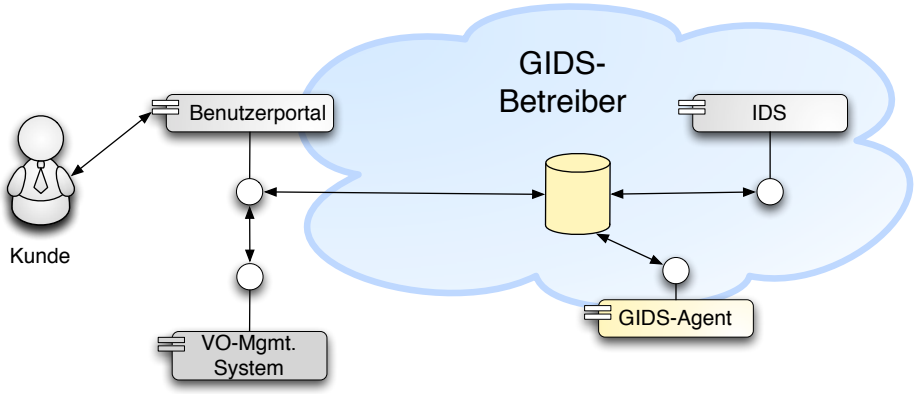


Abbildung 3.2: Architekturüberblick auf Seiten des Betreibers des GIDS

die Hauptaufgabe des GIDS-Agenten den Datenspeicher mit Informationen, die von den anderen Partnern zur Analyse publiziert werden, zu füllen. Zusätzlich versendet er Grid-global erkannte Angriffe, die durch die entsprechende GIDS-Instanz erkannt wurden. In der Regel stellt der GIDS-Agent die einzige Datenquelle für den Betreiber des GIDS dar. Eine mögliche Ausnahme ist in Abschnitt 3.2.1 aufgezeigt.

Durch die Gleichheit mit dem GIDS-Agenten und Datenspeicher auf Seiten eines Ressourcenanbieters bedingt wird nachfolgend nicht näher auf diese Komponenten eingegangen. Für eine genauere Beschreibung sei auf den Abschnitt 3.1.1 verwiesen.

Grid-globale GIDS-Instanz. Der Grid-globalen Instanz zur Auswertung der im Grid verfügbaren Informationen stehen in der Regel die wenigsten Originalinformationen zur Analyse zur Verfügung. Dies liegt daran, dass in der zugehörigen Informationsbasis ausschließlich die im Grid „öffentlich“ verfügbaren Daten, die von den beteiligten GIDS-Agenten publiziert worden sind, verfügbar sind. Diese Informationen sind bereits von den jeweiligen Ressourcenanbietern gefiltert, aggregiert und verdichtet sowie anonymisiert und/oder pseudonymisiert worden (siehe auch Abschnitt 3.1.1). Daraus folgt, dass dieser Instanz des IDS nur eine Teilmenge der Informationen vorliegt, die paarweise jedem einzelnen Ressourcenanbieter zur Verfügung steht. Es ist also zu erwarten, dass die Grid-globale GIDS-Instanz in Bezug auf ihre Erkennungsleistung gegenüber den jeweils lokalen (G)IDS-Instanzen schlechter abschneidet. Aus diesem Grund erscheint es sinnvoll, dass auch durch (G)IDS-Instanzen erkannte Angriffe durch die Ressourcenanbieter Grid-global publiziert werden, wie auch konzeptuell in Abschnitt 3.1.1 vorgesehen.

Benutzerportal. Auf Basis der in der Datenbank hinterlegten Berichte stellt das Benutzerportal eine mandantenfähige Nutzeroberfläche zur Berichterstattung bereit. Nutzer (Mitglieder einer VO oder auch Ressourcenanbieter) können hier den aktuellen Sicherheitsstatus des Grids unter Nutzung ihrer im Grid gültigen Credentials einsehen sowie historische Berichte anfragen. Es werden verschiedene Sichten auf die Berichte je nach Rolle des Nutzers angeboten.

Da das Benutzerportal auf der einen Seite nur Abhängigkeiten von bestehenden Grid-Diensten und auf der anderen Seite von einer GIDS-Datenbank hat, kann es auch zum Betrieb bei einem beliebigen anderen Teilnehmer des GIDS verwendet werden. Dadurch kann eine redundante Auslegung bzw. eine Wiederverwendung dieser Komponente als Managementoberfläche bei den Ressourcenanbietern ermöglicht werden.

Proaktive Benachrichtigung. Diese Komponente dient dazu die Kunden des GIDS, also sowohl Mitglieder einer VO als auch Ressourcenanbieter, über die aktuelle Sicherheitslage stets proaktiv, d.h. sofort nach erkanntem Angriff, in Kenntnis zu setzen. Dies kann auf

verschiedenen Kommunikationswegen wie z.B. E-Mail oder SMS geschehen. Eine Auswahl des Kommunikationskanals kann in Abhängigkeit der Wichtigkeit einer Nachricht erfolgen.

Genau wie für das Nutzerportal auch, bestehen für die Komponente der proaktiven Benachrichtigung nur Abhängigkeiten zu bestehenden Grid-Diensten und einer GIDS-Datenbank. In hiesigem Fall ist die Anbindung an eine Datenbank zur Abbildung von Ressourcen auf die sie nutzenden VOs sowie an das VO-Managementsystem zum Bezug der Kontaktdaten der jeweils verantwortlichen Personen notwendig. Somit kann auch diese Komponente bei einem beliebigen anderen Teilnehmer des GIDS betrieben werden.

3.2 Weitere Rollen im GIDS

Dieser Abschnitt betrachtet kurz weitere Rollen, die im Rahmen des GIDS einen Ausschlag geben werden. Insbesondere gehen die Teilabschnitte dabei auf die Rolle von Drittanbietern, Analysten sowie Kunden eines potentiellen GIDS-Dienstes ein.

3.2.1 Drittanbieter

In den bisherigen Abschnitten stand insbesondere die Konzeption und Inbetriebnahme eines Intrusion Detection Systems für Grids im Vordergrund. Betrachtet man jedoch einen Dienstlebenszyklus, so ist auch die Adaption des Dienstes während seiner Betriebsphase integraler Bestandteil. Hierzu soll in diesem Abschnitt die Möglichkeit der Erweiterung des zuvor konzipierten GIDS kurz beleuchtet werden. Die Erweiterungsmöglichkeiten zeigen sich dabei zweidimensional, zum einen kann das GIDS um weitere Informationsanbieter aus dem Grid (zum Beispiel zusätzliche/neue Ressourcenanbieter) ergänzt werden, zum anderen können auch Informationen von dem Grid fremden Drittanbietern dienlich beigesteuert werden. Diese beiden Fälle werden nachfolgend kurz detailliert.

Erweiterung um weitere Informationsanbieter aus dem Grid

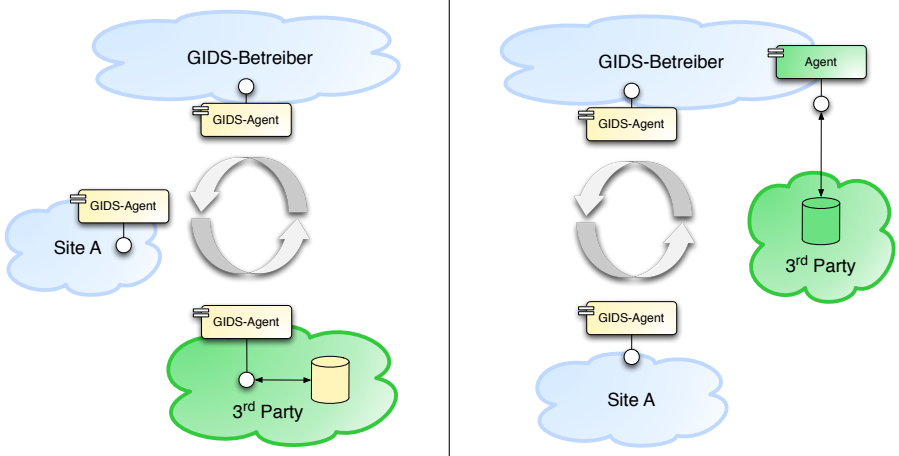
Die einzig notwendige Vorraussetzung, um einen weiteren Informationsanbieter in das GIDS zu integrieren, ist, dass dieser einen GIDS-Agenten zur Kommunikation innerhalb des GIDS in Betrieb nimmt. Dieser neue GIDS-Agent muss dazu autorisiert werden, am Datenaustausch teilzunehmen, was durch die koordinierende Instanz, also den GIDS-Betreiber, Grid-global vorgenommen werden kann. Prinzipiell kann diese Funktion jedoch ein beliebiger vertrauenswürdiger Teilnehmer des GIDS übernehmen.

Damit der neue Informationsanbieter die anfallenden Daten, die im GIDS verteilt werden, sinnvoll nutzen kann, muss er mindestens eine lokale Instanz eines (G)IDS mit einer angeschlossenen Datenbank vorhalten. Um auch aktiv Sensordaten und Sicherheitsberichte im Grid verbreiten zu können, sind zusätzlich Agenten an den lokal datensammelnden Komponenten zu platzieren sowie die Kaskade an Komponenten, die eine geregelte Datenweitergabe gewährleistet (*Filter*, *Aggregator* und *Anonymisierer/Pseudonymisierer*), zu etablieren.

Erweiterung um Informationen von Drittanbietern

Die in Abschnitt 2 vorgestellte Idee zum Aufbau eines Grid-weiten Frühwarnsystems in der Art und Weise, wie es vorgeschlagen ist, bietet insbesondere die Möglichkeit der Erweiterung der Informationsbasis durch das Hinzufügen weiterer Informationsanbieter. Wie auch in der Anforderungsanalyse deutlich geworden ist, können durchaus auch Informationen von Drittanbietern wie beispielsweise CERTs von großem Interesse sein. Da ein durch die Vernetzung der GIDS-Agenten bedingtes Informationsverbreitungssystem besteht, ist es denkbar, auch externe Informationsquellen, die als vertrauenswürdig und hilfreich eingestuft werden, mit einzubinden.

Dies geschieht zum Beispiel durch die Installation eines entsprechenden Agenten direkt beim Informationsanbieter, wie es in Abbildung 3.3a graphisch dargestellt wird. Dies hat jedoch unter anderem den Nachteil, dass eine im Grid nicht beteiligte Partei (in diesem Fall



(a) direkt (b) via Mittelsmann

Abbildung 3.3: Erweiterung des GIDS um Informationen von Drittanbietern

also der Drittanbieter) konzeptuell alle Informationen, die die am GIDS beteiligten Partner untereinander austauschen, mithören kann. Dies kann aus verschiedenen Gesichtspunkten (mangelndes Vertrauen, juristische Einschränkungen etc.) nicht erwünscht oder erlaubt sein.

Alternativ kann eine Anbindung über einen Mittelsmann im Grid, der die Informationen für das GIDS aufbereitet und bereitstellt, geschehen (siehe Abbildung 3.3b). Ein geeigneter Mittelsmann dafür ist beispielsweise der geforderte Betreiber des GIDS. Dieser kann unter Nutzung eines eigenen Agenten die Informationen des Drittanbieters entgegennehmen, aufbereiten und in seiner Informationsbasis hinterlegen. In Abweichung zu dem zuvor beschriebenem Fakt, dass der Betreiber des GIDS sich unter anderem von einem Ressourcenanbieter darin unterscheidet, dass er nicht als Informationsanbieter fungiert, stellt in diesem Fall der Betreiber des GIDS doch Informationen im GIDS bereit.

3.2.2 Analysten

Bei der Erkennung von Angriffen muss man zwei Szenarien unterscheiden. Das einfachere Szenario ist die Erkennung von bekannten Angriffen oder von Varianten bekannter Angriffe. Da jeder Angriff im Allgemeinen eine charakteristische Eigenschaften aufweist, kann man über signaturbasierte Analysefunktionen diese Angriffe automatisch erkennen. Zwar entfällt in diesem Fall eine separate Analyserolle, jedoch ist diese für andere Szenarien notwendig.

Das deutlich aufwändigere Szenario besteht in der Analyse und Erkennung von bisher unbekannten Angriffen oder sehr starken Variationen bekannter Angriffe. Da hierbei die Charakteristiken nicht bekannt sind, ist eine automatische Analyse der Bedrohungslage automatisiert sehr schwer nur möglich. In [2] wird diese Problematik verdeutlicht. Weiterhin versuchen die Autoren, diesem Umstand Rechnung zu tragen, indem sie Hintergrundwissen in die Analyseeinheit mit einfließen lassen. Ohne Hintergrundwissen ist es einer automatisierten Analyseeinheit jedoch nur möglich, eine Abweichung vom Normalzustand zu melden. Diese Meldung ist jedoch potentiell ein *false positive* und kann daher nicht ohne weitere Analyseschritte an die Kunden oder Ressourcenprovider gemeldet werden.

Die aus diesem Grund nötige Analystenrolle kann nun entweder bei den Ressourcenprovidern oder beim GIDS-Betreiber angesiedelt sein. Im ersten Fall hat der Analyst den Vorteil, dass er seine Untersuchungen auf eine größere Datenbasis stützen kann, da er auch auf Datensätze zugreifen kann, die bei seinem Provider anfallen, aber durch den *Filter* aussortiert werden. Der Nachteil an dieser Konstellation ist, dass es nötig ist, dass mehrere verschiedene Ressourcenanbieter je eine eigene Analystenrolle anbieten, um zum einen die Ausfallsicherheit zu gewährleisten und zum anderen, um die Abhängigkeit von einem Provider zu minimieren.

Die Analystenrolle kann aber auch vom GIDS-Betreiber angeboten werden oder gegebe-

nenfalls von diesem an externe Dienstleister ausgelagert werden. Da in Abschnitt 3.2.1 auch schon eine Anbindung des GIDS-Betreibers an CERTs angesprochen wurde, und diese über neue Bedrohungen und Angriffsmuster in den meisten Fällen sehr früh informiert sind, ist eine Zusammenarbeit im Bereich der Früherkennung von bisher unbekannten Angriffen möglich.

3.2.3 Kunden

Ein zentraler Bestandteil von Grids ist das Konzept der Virtuellen Organisation (VO). In der Literatur findet sich eine Vielzahl verschiedener, jeweils auf den speziellen Anwendungsfall hin zugeschnittene Definitionen. Für diese Arbeit wird daher im Folgenden die Definition einer VO nach [8] herangezogen:

> **Definition (Virtuelle Organisation):** Eine Virtuelle Organisation ist eine zeitlich begrenzte koordinierte Kooperation von Elementen in Form von Individuen, Gruppen von Individuen, Organisationseinheiten oder ganzer Organisationen, die Teile ihrer physischen oder logischen Ressourcen oder Dienste auf diesen, ihre Kenntnisse und Fähigkeiten sowie Teile ihrer Informationsbasis in Form virtueller Ressourcen und Dienste über eine Grid-Infrastruktur derart zur Verfügung stellen, dass die gemeinsam vereinbarten Ziele unter Berücksichtigung lokaler und globaler Policies erreicht werden können.

Insbesondere das Management dynamischer, interorganisationaler Virtuellen Organisationen stellt immense Herausforderungen dar. Um diesen zu begegnen, bedarf es neuer Ideen und Technologien, die unter anderem in [8] behandelt werden. In der heutigen Praxis wird zumeist im Zusammenhang mit dem Management von VOs nur eine Infrastruktur zur Authentifizierung und Autorisierung von Nutzern (eine sogenannte AA-Infrastruktur oder auch einfach nur AAI) beschrieben. Im Grid-Umfeld kommt hierzu zum Beispiel Shibboleth (`http://shibboleth.internet2.edu/`) zum Einsatz, auf dessen Konzepte und Komponenten an dieser Stelle nicht weiter eingegangen werden soll.

Aus der speziellen Rolle der VOs wurden schon mehrere Anforderungen erhoben, wie beispielsweise verschiedene Granularitätsstufen der Berichterstattung oder die Anbindung von bestehenden VO-Managementsystemen. Mit diesen Anforderungen soll garantiert werden, dass Mitglieder einer VO, die zwar die Berechtigung haben, die Ressourcen eines Providers zu verwenden, nicht unbedingt alle Warn- beziehungsweise Alarmmeldungen des Providers zu sehen bekommen, sondern der Provider selbst entscheiden kann, welche VOs welche Informationen bekommen. Die Berichte für die Kunden von GIDS können zum einen im *Benutzerportal* abgerufen werden oder die Kunden können auch *proaktiv benachrichtigt* werden, wie in Abschnitt 3.1.2 beschrieben.

3.3 Nutzbare Design-Patterns

Entwurfsmuster (oder english *design patterns*) [3] sind bewährte Lösungsvorlagen für wiederholt auftretende Entwurfsprobleme aus dem Objekt-Orientierten Software-Entwurf. Hierfür existieren für verschiedene Problemstellungen eine Vielzahl unterschiedlicher Entwurfsmuster, die auch auf ihre Anwendbarkeit zur Implementierung der zuvor stehend genannten GIDS-Komponeten geprüft werden sollen. Im Rahmen dieser Arbeit betrachten wir kurz die Entwurfsmuster *Adapter Pattern* oder auch *Wrapper Pattern*, *Observer Pattern* oder auch bekannt als *Publish-Subscribe Pattern* oder *Dependents Pattern* und das *Bridge Pattern*.

Adapter Pattern. Die Aufgabe des *Adapter Pattern*, das auch oftmals als *Wrapper Pattern* bezeichnet wird, ist eine Übersetzung einer Programmschnittstelle in eine nicht trivial kompatible andere Programmschnittstelle. Dadurch kann erzielt werden, dass ursprünglich inkompatible Klassen durch den Einsatz eines Adapters eine Kompatibilität zueinander erzielen. Um dieses Ziel zu erreichen, wird die ursprüngliche Programmschnittstelle einer Klasse A, die mit einer anderen Klasse B zusammenarbeiten soll, verwendet, um die von der Klasse B erwartete Schnittstelle zu realisieren. Als Beispiel

könnte die Abbildung einer Integer-Zahl auf eine Fließkommazahl durch einen Adapter vorgenommen werden. Der Vorgang der Anpassung einer Programmschnittstelle ist jedoch im Gegensatz zum zuvor genannten Beispiel in den meisten Fällen nicht trivial. So ist z.B. der umgekehrte Vorgang der Abbildung einer Fließkommazahl auf einen Integer-Wert diskussionsfähig und mit hoher Wahrscheinlichkeit mit einem Informationsverlust behaftet.

Observer Pattern. Für die Umsetzung der GIDS-Agenten bietet sich ggf. die Verwendung des *Observer Pattern* (auch bekannt als *Publish-Subscribe Pattern* oder *Dependents Pattern*) [3] an. Das Observer Pattern definiert dabei eine $1 : n$-Beziehung zwischen den GIDS-Agenten. Es ist dazu intendiert, dass, wenn sich der Zustand eines der Objekte ändert, alle anderen Objekte automatisch über diese Änderung informiert werden. Im Fall der GIDS-Agenten bedeutet dies, dass, wenn einer der GIDS-Agenten einen Datensatz zur Informationsverbreitung erhält (dies entspricht also der Zustandsänderung), so informiert er alle weiteren GIDS-Agenten über den Eingang dieses Datensatzes. Einen möglichen Ansatz zur Einführung des Publisher-Subscriber Design Pattern in Infrastrukturen verteilter IDS beschreiben Basicevic et. al. in [1].

Bridge Pattern. Eine Orientierung an dem sogenannten *Bridge Pattern* nach [3] eignet sich beispielsweise zur Implementierung des Benutzerportals. Hierdurch kann erreicht werden, dass die Abstraktion des Benutzerportals von seiner Implementierung vollkommen losgelöst ist. Im Gegensatz zu regulären Vererbungen wird durch den Einsatz des Bridge Pattern eine harte Bindung von Abstraktion und Implementierung vermieden, so dass sowohl die Abstraktion, als auch die Implementierung durch Unterklassen erweiterbar bleiben, während dies keinen Einfluss auf nachgelagerte Anwendungen hat.

Kapitel 4

Abhängigkeiten

In diesem Abschnitt sollen Abhängigkeiten zwischen der vorgestellten Grobarchitektur und verschiedenen Komponenten des entstehenden GIDS dargestellt werden. Einerseits müssen durch die entwickelte Architektur Anforderungen der anderen Komponenten erfüllt werden. Andererseits ist zu berücksichtigen, dass die erforderlichen Funktionalitäten der entstehenden Gesamtinfrastruktur durch die in diesem Grobkonzept vorgestellte Architektur erfüllt werden können.

4.1 Informationsmodell und Datenaustauschformat

Zwei der zu berücksichtigenden Abhängigkeiten für das Grobkonzept der Architektur sind die Konzeption des Informationsmodells und die Wahl des Datenaustauschformats. Im Folgenden wird erläutert, wie sich die Abhängigkeiten darstellen und was bei der Entwicklung – sowohl des Grobkonzepts, als auch der jeweiligen Komponente – zu beachten ist, um die Erfüllung der Anforderungen sicherzustellen.

4.1.1 Sicherheit bei der Informationsübertragung

Beim Informationsmodell wie auch beim Datenaustausch muss unterschieden werden zwischen dem Site-lokalen und dem Grid-globalen Austausch von Informationen. Während die Site-lokale Kommunikation meist in einem geschützten, nicht öffentlichen Netzwerk stattfindet, muss bei der Grid-globalen Kommunikation, bedingt durch die geografische Verteilung der Systeme, von der Nutzung öffentlicher Netze ausgegangen werden. Entsprechende Sicherheitsvorkehrungen zur Wahrung der Vertraulichkeit und der Integrität müssen bei beiden Arten umgesetzt werden. Sowohl zwischen lokalen GIDS-Komponenten wie Sensoren, Agenten und Datenbanken, als auch zwischen den autonomen Einzelsystemen des GIDS auf Seiten der Ressourcenanbieter, dem GIDS-Betreiber und den Kunden des GIDS muss für die Sicherheit der Daten gesorgt werden.

4.1.2 Effiziente Datenübermittlung und -verarbeitung

Während des normalen Betriebs des GIDS sind bei jedem Provider des Grids verschiedenste Agenten zur Sammlung von Informationen über etwaige Angriffe tätig. Diese Agenten können je nach Art des Sensors sehr viele Daten liefern. Zum einen muss ein Datenaustauschformat gefunden werden, welches trotz der großen Datenmengen effizient arbeitet und trotzdem die oben genannten Sicherheitsmechanismen bietet. Auch hierbei ist zwischen der Site-lokalen und der Grid-globalen Kommunikation zu unterscheiden. Site-lokal werden wesentlich größere Datenmengen durch die ungefilterte Übertragung zum GIDS-System anfallen, als bei der Übertragung von gefilterten und angereicherten Informationen zum GIDS-Betreiber.

Neben der lokalen und Grid-weiten Übermittlung von GIDS-Daten ist die effiziente Verarbeitung auf den lokalen GIDS-Systemen entscheidend. Bei der lokalen Verarbeitung der Daten auf Seiten der Ressourcen-Provider fallen Aufgaben wie das Ausfiltern unbrauchbarer und

redundanter Informationen, die Aggregation und Korrelation bestimmter Ereignisse und auch die Anonymisierung an. Durch ein entsprechend zu entwickelndes Informationsmodell und geschickte Aggregation der Daten muss hierbei die effiziente Verarbeitung sichergestellt werden. Auch auf Seiten des GIDS-Betreibers muss die effiziente Verarbeitung der Daten durch das Informationsmodell sichergestellt werden.

4.1.3 Sichere Datenhaltung

Die für eine Angriffserkennung erforderlichen Daten werden, wie in diesem Grobkonzept beschrieben, an mehreren Stellen verteilt gespeichert. Zum einen befinden sich lokale Daten in den lokalen GIDS-Datenbanken. Hier befinden sich sensible Daten, die keinesfalls in die Hände Dritter gelangen dürfen. Mitunter werden Daten gespeichert, die die Heimatorganisation nicht verlassen sollen oder sogar dürfen. Der Schutz der Privatssphäre der Benutzer und entsprechend der Daten ist gesetzlich geregelt. Ein erster Ansatz zum Schutz der Daten wäre es, die Daten ausreichend stark verschlüsselt abzulegen. Hierbei ist zu beachten, dass die Performanz der GIDS-Komponenten nicht maßgeblich unter der zusätzlichen Belastung durch Ver- und Entschlüsselung leidet.

Neben den oben genannten Daten der Betreiber sind die gesammelten, zusammengefassten und aggregierten Daten auf Seiten des GIDS-Betreibers ebenfalls durch kryptografische Methoden zu schützen. Nur durch die Kombination von einer verschlüsselten Datenhaltung zusammen mit einer gesicherten Übertragung der Daten an andere GIDS-Teilnehmer kann die korrekte Funktionsweise des GIDS gesichert werden.

Eine wichtige Frage bei der Datenhaltung ist die Zeitspanne, nach der die Daten gelöscht werden müssen. Gerade bei personenbezogenen Daten gibt es gesetzliche Auflagen, die maximale Aufbewahrungsfristen vorschreiben. Diese Frage sollte innerhalb des künftigen Datenschutzkonzepts geklärt werden. Aber auch bei datenschutzrechtlich unbedenklichen Daten ist es sinnvoll, wenn Daten nicht unbegrenzt gespeichert werden, um einen zukünftigen Missbrauch vorzubeugen.

4.1.4 Datenformat

Das Datenaustauschformat, welches bei der Kommunikation zwischen den einzelnen GIDS-Komponenten eingesetzt wird, muss den Anforderungen des Datenschutzkonzepts entsprechen. Diese werden in einem gesonderten Meilenstein erarbeitet und im folgenden Abschnitt 4.2 kurz erläutert.

Die Sammlung von Informationen auf Seiten der GIDS-Provider geschieht über die Einbindung verschiedenster Sensoren. Durch die verschiedenartigen Sensoren werden sehr heterogene Informationen gesammelt. Die entstehende offene Architektur sowie die angestrebte Autonomie der einzelnen GIDS-Provider erfordern ein flexibles Datenformat. Eine mögliche und bereits existierende Lösung stellt das Intrusion Detection Message Exchange Format (IDMEF) [5] dar. Auf die Verwendung von IDMEF im GIDS-Projekt wird in Kapitel 5 eingegangen.

4.2 Datenschutzkonzept

Während das Informationsmodell und Datenaustauschformat die technischen Aspekte der Speicherung und des Austausch der GIDS Daten betrachtet, bestimmt das Datenschutzkonzept die technischen, organisatorischen und rechtlichen Aspekte zum Schutz der Daten. Diese betreffen speziell die Speicherung, Verwertung und den Austausch von personenbezogenen Daten sowie deren Anonymisierung oder Pseudonymisierung, falls dies notwendig oder gewünscht ist.

Die Anforderungen an das Datenschutzkonzept, die sich aus denen des Grid-IDS (*GIDS*) ergeben, sind bereits im Kapitel 3.1 genannt worden. Daneben ergeben sich aber noch weitere organisatorische und rechtliche Aspekte, die sich aus gesetzlichen Zwängen und anderen Grundlagen ableiten. In diesem Abschnitt wird kurz auf die grundlegenden Abhängigkeiten des Datenschutzkonzeptes mit dem Konzept des GIDS eingegangen, in dem die grobe Architektur und Rollen beschrieben werden. Neben der Unterstützung der in Kapitel 3.1 aufgestellten

Anforderungen basiert das Datenschutzkonzept auf weiteren Grundlagen, die Abhängigkeiten nach sich ziehen:

Least Privilege In der Informationssicherheit besagt dieses Prinzip, dass der Zugriff und Verteilung von Daten auf das Notwendige zu beschränken ist. Auf der einen Seite ist es erstrebenswert, möglichst viele Informationen zu erheben und allen Seiten offen zur Verfügung zu stellen. Zwar unterstützt dies die Erkennung von Angriffen, jedoch entstehen auf der anderen Seite durch einen zu freizügigen Umgang mit den Daten auch neue Risiken:

- Angreifer können durch den offenen Umgang mit Daten leichter in den Besitz von kritischen Informationen gelangen. Dies können Angriffsdaten oder administrative Daten eines Ressourcenzulieferers sein.
- Es besteht die Gefahr, dass Daten unbeabsichtigt aus dem Einflussbereich des GIDS heraussickern.
- Es ist schwierig, die Übersicht zu behalten, welche Benutzer auf welche Daten Zugriff haben und diese vorrätig halten.
- Weiterhin bestehen rechtliche Einschränkungen der Speicherung und Verwendung personenbezogener Daten, die berücksichtigt werden müssen.

Die Risiken werden durch das *Least Privilege* Prinzip reduziert, indem die Verbreitung und Offenlegung der Daten auf das Notwendige reduziert. Beispielsweise ist es für die Erkennung der Angriffe nicht unbedingt notwendig, dass die IP-Adressen und Benutzernamen im Klartext vorliegen. Hierfür reichen in der Regel pseudonymisierte Daten, womit eine Korrelation zur Erkennung von Angriffsszenarien weiterhin möglich ist. Konkrete Abhängigkeiten ergeben sich durch die Wahl der Rollen und die technischen Komponenten zur Filterung, Aggregierung und Anonymisierung der Daten. Es ergeben sich insbesondere Abhängigkeiten durch die Aufgaben der Rollen und deren Abhängigkeiten und Workflows untereinander. Hierbei sind die folgenden Punkte zu berücksichtigen:

- Aus den **Aufgaben** der Rollen ergibt sich, welche Daten diese benötigt und in welcher Form diese Daten verarbeitet werden und vorliegen müssen. Wie bereits vorher erwähnt sind pseudonymisierte Daten häufig vollkommen ausreichend.
- Es gibt verschiedene **Abhängigkeiten** und **Workflows** zwischen den Rollen. Dies betrifft den Transport und Schutz der Daten. Soll beispielsweise eine Kooperation mit einem CERT zur Nutzung der Daten für die Vorfallsbearbeitung etabliert werden, ist das Aufheben der Pseudonymisierung in speziellen Fällen erforderlich.
- Weiterhin ist die Gewährleistung eines sicheren Zugriff auf die Daten ein wichtiger Aspekt des Datenschutzes. Dies erfordert ein geeignetes Verfahren zur Authentifizierung und Autorisierung der Rollen. Dies ist insbesondere kritisch, wenn die Zuordnung von Individuen zu den Rollen wie bei Grids dynamischen Änderungen unterliegt.

Rechtliche Konformität Das GIDS erhebt kritische Daten, die sowohl Angriffe als auch administrative Daten der beteiligten Seiten beinhalten. Diese Daten haben teilweise Bezug zu Personen und unterliegen deshalb den gesetzlichen Auflagen. Zwar ist die Erhebung, Verarbeitung und Weitergabe dieser Daten grundsätzlich möglich, sie unterliegen aber starken gesetzlichen Einschränkungen. Diese müssen natürlich bei der Konzeption des Datenschutzkonzeptes berücksichtigt werden. Für diesen Punkt sind wieder die Aufgaben und Abhängigkeiten der Rollen von Bedeutung. Weiterhin ist zu berücksichtigen, wie die Daten erhoben worden sind und aus welchen Quellen diese stammen. In diesem Zusammenhang ist zu unterscheiden, ob die Daten direkt Angriffen zugeordnet sind oder nicht. Im ersten Fall sind die Daten anlassbezogen – beziehen sich also auf einen konkreten Angriff – und werden benötigt, um diese Störung – den Angriff – einzugrenzen und zu beheben. Damit dienen die Daten zur Behebung von Störungen und es bieten sich andere rechtliche Möglichkeiten als wenn die Daten ohne Anlass gesammelt werden. Zusammenfassend ergeben sich die folgenden Abhängigkeiten:

- Aus der Sensorik ergibt sich, welche Daten in welcher Form erhoben werden und welcher Personenbezug in den Daten vorhanden ist. Daraus kann dann beispielsweise abgeleitet werden, ob die Daten in der Rohform weitergeleitet werden können, oder ob sie anonymisiert oder pseudonymisiert werden müssen.
- Aus den Rollen und deren Aufgaben und Workflows kann der Verwendungszweck der Daten abgeleitet werden. Wie bereits oben beschrieben beeinflusst der Verwendungszweck die Einschränkungen für die Erhebung und Weitergabe der Daten. Weiterhin bildet dieses Wissen die Grundlage, welche Daten anonymisiert beziehungsweise pseudonymisiert werden müssen und an welcher Stelle dies geschehen muß.

Bedürfnisse der teilnehmenden Seiten Am GIDS sind neben Ressourcenanbietern auch weitere Seiten beteiligt. Diese können beispielsweise Kunden und CERTs sein. Jeder dieser am GIDS beteiligten Seiten hat ihre eigenen Bedürfnisse, die von dem Datenschutzkonzept in Beziehung stehen.

Um die Bedürfnisse der teilnehmenden Ressourcenprovider im Vorfeld abschätzen zu können, wurde zu Beginn des Projekts in Arbeitspaket 1 eine Umfrage unter allen D-Grid Sites durchgeführt. Die Auswertung der Umfrage ist Teil des Meilensteinberichts [7].

Eine wichtige Forderung des GIDS-Konzeptes ist die Autonomie der Ressourcenanbieter. Dies betrifft auch die Daten, die die beteiligten Partner an das GIDS liefern. Dabei hat die Erfahrung gezeigt, dass Ressourcenanbieter häufig sehr zögerlich sind, kritische Informationen herauszugeben. Befürchtungen sind, dass Dritte Aufschlüsse über aktuelle Sicherheitsprobleme in deren Netzwerk erhalten. Ein weiterer Grund ist der Zwang der Rechtfertigung gegenüber den Benutzern, dass deren Daten weitergegeben werden. Daraus ergeben sich neben den rechtlichen weitere Gründe, Daten zu filtern oder zu anonymisieren. Diese Bedürfnisse können beispielsweise durch eine Kooperationsvereinbarung geregelt werden, die Teil des Datenschutzkonzeptes ist.

Wir haben in unserer Umfrage unter anderem festgestellt, dass etwa ein Drittel der teilnehmenden Sites keine Netflow-Daten aufzeichnet. Da die Analyse von Netflow-Daten zur Erkennung von vielen Angriffen sehr hilfreich ist, ist es nötig, zu erfahren, warum die betroffenen Sites auf dieses Hilfsmittel verzichten oder unter welchen Bedingungen eine Auswertung, auch wenn sie mit Einschränkungen verbunden ist, trotzdem möglich gemacht werden kann.

Damit hat das Datenschutzkonzept zusammenfassend die Aufgabe auf der Grundlage der Architektur und den Rollen des IDS allen Anforderungen gerecht zu werden. Das betrifft sowohl die technischen Komponenten zur Filterung und Anonymisierung bzw. Pseudonymisierung der Daten als auch die organisatorischen Aspekte. Letztere beinhalten Vereinbarungen zwischen den Partnern über die Erhebung, Weitergabe und Verwendung der Daten.

Kapitel 5

Implementierungsmöglichkeiten für einzelne Komponenten

Dieses Kapitel gibt eine erste Übersicht und Vorschläge für die mögliche Implementierung einzelner Komponenten, die bereits im Grobkonzept eines IDS für das D-Grid in Kapitel 2 hervorgebracht worden sind. Dabei werden insbesondere die Konzepte der jeweiligen Implementierung, sowie Möglichkeiten und Probleme der einzelnen Ansätze betrachtet. In Kapitel 5.5 wird schließlich noch eine Grobübersicht eines zukünftigen Integrationskonzepts gegeben.

5.1 Geschützte Kommunikation durch OpenVPN

Wie bereits in Kapitel 4 beschrieben ist eine sehr wichtige Anforderung an die Infrastruktur des GIDS-Dienstes, dass vertrauliche Informationen (mit zum Teil privaten Daten) über unsichere Medien transportiert werden müssen. Hierfür gilt es eine Lösung zu finden, die einerseits die Sicherheit der Daten gewährleisten und andererseits alle Anforderungen, die sich durch die Infrastruktur selbst ergeben, erfüllen kann. Im Folgenden wird das OpenVPN-Projekt [11] betrachtet als eine mögliche Realisierung geschützter Kommunikation zwischen den GIDS-Agenten, GIDS-Kunden und dem GIDS-Betreiber.

Über ein *Virtual Private Network* (VPN) können zwei oder mehr private Netze miteinander verbunden werden. Durch die Verwendung von kryptografischen Verfahren erfolgt die Kommunikation verschlüsselt. Somit kann man allein durch Software ein sicheres, privates Netzwerk auch auf unsicheren Leitungen bereitstellen. In Bezug auf das GIDS-Projekt wäre die Realisierung des GIDS-Bus mithilfe dieser Technik denkbar.

Neben finanziellen Aspekten sind die technischen und entscheidenden Vorteile die Möglichkeit der Authentifikation über X.509-Zertifikate, die Broad- und Multicast-Fähigkeit und das in Version 2.1 eingeführte Port-Sharing. Bei einer Lösung mithilfe von OpenVPN ergeben sich leider auch Nachteile, wie zum Beispiel einen zentralen Server als Single Point of Failure. Diese Vor- und Nachteile sollen im folgenden kurz erläutert werden.

Opensource OpenVPN bietet einige Vorteile bei der Konzeption und Realisierung der Infrastruktur für ein Grid-basiertes Intrusion Detection System. Bei OpenVPN handelt es sich um ein Opensource-Projekt. Entsprechend fallen für GIDS bei der Nutzung der Community-Version von OpenVPN keine Kosten an. Weiterhin ist durch die Quelloffenheit gesichert, dass eine Weiterentwicklung der Software auch nach Ausscheiden des Hauptentwicklers noch möglich ist.

Authentifizierung mittels X.509-Zertifikaten Um die Kommunikation durch ein VPN absichern zu können, ist beim Verbindungsaufbau eine Authentifizierung durchzuführen. Sowohl der Server als auch der jeweilige Client müssen sicher davon ausgehen können, dass es sich beim entsprechenden Kommunikationspartner zum einen nicht um einen Angreifer handelt und zum anderen um genau das System, an das die vertraulichen Daten

auch übertragen werden sollen. Im D-Grid werden zur Authentifizierung bei der Abgabe von Gridjobs und zur verschlüsselten Kommunikation sogenannte X.509-Zertifikate verwendet [4]. Hierbei handelt es sich um von einer *Certificate Authority* (CA) ausgestellte (signierte) Zertifikate, mithilfe welcher ein öffentlicher Schlüssel eindeutig einer Entität (Benutzer/Host) im Grid zugeordnet werden kann. Die gesicherte Kommunikation setzt voraus, dass alle im Grid verwendeten Zertifikate von einer CA ausgestellt (also signiert) werden, denen alle Gridressourcen explizit ihr Vertrauen aussprechen. OpenVPN erlaubt zum Aufbau einer authentifizierten Verbindung zum OpenVPN Access Server ebenfalls X.509-Zertifikate. Die bestehende Authentifizierungsstruktur kann also ebenfalls für den GIDS-Dienst verwendet werden.

Broadcast- und Multicast-Nachrichten Die sichere Verteilung von Informationen zwischen den GIDS-Agenten und dem GIDS-Provider ist ein wesentlicher Bestandteil der GIDS-Infrastruktur. Informationen müssen nicht nur von den GIDS-Agenten an einen zentralen GIDS-Provider übermittelt werden. Eine wesentlich größere Herausforderung stellt die Übermittlung von allgemeinen Informationen an alle beteiligten GIDS-Agenten dar. Allgemeine Informationen können beispielsweise aus einer Warnung über einen aktuellen Angriff bestehen, der so auf anderen Gridressourcen proaktiv verhindert werden kann. Die Übermittlung von Daten an mehr als einen Empfänger könnte mittels OpenVPN über Broadcast-Nachrichten erfolgen. Unter der Voraussetzung, dass dem zentralen GIDS-Betreiber alle beteiligten GIDS-Agenten bekannt sind, wäre auch die Verwendung von Multicast-Nachrichten denkbar.

Port-Sharing Das seit Version 2.1 in OpenVPN eingeführte Feature *Port-Sharing* erlaubt es, den selben Port sowohl für *HTTP over SSL* (HTTPS), als auch für den VPN-Dienst bereit zu stellen. Die Verwendung des gleichen Ports für beide Dienste ist vor allem für die Administration vorteilhaft. Die bereits konfigurierten Firewallregeln müssen nicht geändert werden. Insbesondere müssen keine weiteren Ports geöffnet werden, um die korrekte Funktion des Grid-basierten IDS zu ermöglichen.

Zentraler Server als Single Point of Failure Ein Nachteil der sich aus der Nutzung von OpenVPN ergibt, ist die Notwendigkeit eines zentralen OpenVPN Access Servers. Alle Clients, die über den GIDS-Bus Daten austauschen / empfangen wollen, müssen sich hier authentifizieren und ihre Verbindung zum GIDS-VPN aufbauen. Eine zentrale Authentifizierungsstelle erscheint zwar zunächst vorteilhaft, birgt aber die Gefahr eines Single Point of Failure. Ist der OpenVPN Access Server, aus welchen Gründen auch immer, nicht erreichbar, so wird die gesamte Kommunikation des GIDS-Systems nicht mehr möglich sein. Sollte die gesamte Kommunikation in der GIDS-Infrastruktur auf den mit OpenVPN gesicherten Bus ausgelegt sein, so wäre dies ein schwerwiegendes Sicherheitsproblem.

Aus diesem Grund ist eine Fallback-Lösung unumgänglich. Hierfür stehen prinzipiell zwei verschiedene Lösungsansätze zur Verfügung. Einerseits besteht die Möglichkeit einen redundanten, zweiten OpenVPN Access Server bereitzustellen, welcher die Aufgaben des primären Servers nahtlos übernehmen kann. Dieser Server muss, um den gleichzeitigen Ausfall beider Server zu verhindern, auf einer anderen Hardware betrieben werden. Idealerweise befinden sich Primärserver und Fallback-Server nicht im gleichen Netzwerk, im Falle des D-Grid also nicht in der gleichen Site. Auf diese Weise würde selbst der vorrübergehende Verlust einer gesamten Site, z.B. durch Netzwerkprobleme, für das GIDS keine Ausfälle bedeuten. Bei diesem Ansatz könnte die Bereitstellung einer Liste von GIDS-VPN Access Servern (mitsamt den Fallback-Systemen) nötig sein. Andererseits wäre auch die Bereitstellung von Repositories zur Verteilung aktueller GIDS-Daten eine vorrübergehende Lösungsmöglichkeit, sollte der zentrale GIDS-VPN Server ausfallen. Auf die Nutzung von Repositories als Zugriff auf GIDS-relevante Daten und Informationen wird im entsprechenden Abschnitt 5.3 näher eingegangen.

Zusammenfassend bietet OpenVPN einige für GIDS sehr interessante Möglichkeiten. Die Nutzung eines eigenst für die streng vertrauliche Kommunikation zwischen den GIDS-Agenten und

dem GIDS-Betreiber eingerichteten Netzwerks ist zur Wahrung der Privatssphäre der Kunden eine sehr interessante Alternative. Ebenso ist die Verwendung etablierter Authentifizierungsmechanismen ein Vorteil. Einziger bislang bekannter Nachteil ist die Entstehung eines Single Point of Failure beim OpenVPN Access Server. Zwei mögliche Ansätze zur Lösung dieses Problems wurden ebenfalls in diesem Abschnitt angesprochen.

5.2 Peer-2-Peer-gestützte Ansätze zur Kommunikation

Beim Design von Infrastrukturen wird zwischen verschiedenen Ansätzen unterschieden. Als Ziele verfolgen diese Infrastrukturen unter anderem die Robustheit und Effizenz des Austauch von Informationen. Allerdings können beide Ziele als typisches Problem der Optimierung nicht gleichzeitig optimal unterstützt werden. Die Robustheit wird in der Regel durch redundante Kanäle zwischen den Partnern erreicht, die aber die Effizienz in Bezug auf die Menge der zu übertragenden Daten reduziert.

Das Design von Peer-2-Peer Netzwerken zielt meistens auf die Robustheit der Infrastruktur ab. Dabei besteht das Netzwerk in der Regel aus gleichberechtigten Partnern, zwischen denen Daten ausgetauscht werden. Werden die Partner als Knoten und die Kommunikationskanäle als Kanten zwischen je zwei Knoten angesehen, ergibt sich daraus ein Graph. Werden die Daten in beide Richtungen zwischen den Partnern ausgetauscht, ist dies ein ungerichteter Graph, im anderen Fall entsteht ein gerichteter Graph. Damit die Informationen alle Partner erreichen, muss der Graph zusammenhängend sein. Unterschiede liegen aber in der Anzahl und Struktur der Kanten. Im Extremfall können alle Partner mit allen anderen Informationen austauschen. In diesem Fall ist der Graph vollständig vernetzt. Als Vorteil besteht eine maximale Redundanz der Kanäle, die die Architektur extrem robust macht. Es können sehr viele Kanäle ausfallen, ohne dass das Netzwerk zusammenbricht. Als Nachteil ist die Koordination des Datenaustausches sehr aufwendig, um den Mehraufwand bei den versendeten Nachrichten zu minimieren. Trotzdem kann es nicht vermieden werden, dass Nachrichten mehrfach versendet werden, was das Datenvolumen sehr ineffizent macht. Beispielsweise gibt es Ansätze, in denen Daten quasie wie eine Epedemie im Netzwerk verteilt werden. Kritsch ist in diesem Fall allerdings zu entscheiden, wann alle Partner die Informationen erhalten haben und der Versand der Informationen abgebrochen werden kann. Deshalb wird in den meisten Architekturen die Vernetzung begrenzt.

Aufgrund der Robustheit von Peer-2-Peer Netzwerken sind diese bei bösartiger Software (Malware) beliebt. Beispielsweise verwendet das Bot-Netzwerk der Waledac Malware diese Architektur, das beispielsweise in [9] beschrieben wurde. Das Peer-2-Peer Netzwerk ist nicht vollständig vernetzt. Jeder der Waledac Knoten (Repeater) hat eine Liste von Peers, zu den sich dieser verbinden kann.

Peer-2-Peer Netzwerke werden auch für verteilte IDS-Architekturen eingesetzt. Ein erfolgversprechendes Beispiel ist das Domino Overlay System in [14]. Um die Daten der IDS effizient zu verteilen, sieht die Architektur eine ringförmige Struktur von Achsknoten vor, die ein Overlay Netzwerk (Axis Overlay) bilden. Das heißt, über dem Peer-2-Peer Netzwerk wird ein ringförmiges Netzwerk gebildet. Dadurch wird vermieden, dass Nachrichten mehrfach versendet werden müssen. Weiterhin ist das Netzwerk robust gegenüber dem Ausfall eines der Achsknoten. Den Achsknoten hierarchisch untergeordnet sind die „Satellite Communities“. Diese zeichnen Daten über Angriffe auf und geben diese an den übergeordneten Achsknoten weiter. Daneben sieht die Architektur „Terrestrial Contributors“ vor, die allerdings nicht formal in die Architektur eingebunden sind. Dies können beispielsweise Firewalls sein.

Die Kommunikation zwischen den Achsknoten untereinander und den Satellite Communities erfolgt über das Domino Protokoll. Im Gegensatz zu den anderen Komponenten senden die Terrestrial Contributors ihre Daten nicht im Domino Protokoll. Das Domino Protokoll selbst ist eine erweiterte Version des IDMEF.

Obwohl die Domino Architektur viele Gemeinsamkeiten mit der GIDS Architektur hat, lässt sich deren Peer-2-Peer Struktur nicht ohne Weiteres auf das GIDS übertragen. Die

ringförmige Struktur hat viele Gemeinsamkeiten mit einem Bus. Dabei würden die GIDS-Agenten den Achsknoten im Domino System entsprechen. Weiterhin können die Satellite Communities im Domino System analog zu den Sensoren im GIDS sein, die ebenfalls hierarchisch den GIDS Agenten untergeordnet sind. Allerdings setzt das Domino System die Vertrauenswürdigkeit der Achsknoten untereinander voraus. Zwei nicht vertrauenswürdige oder ausgefallene Knoten führen zum Kollaps des Systems. Dagegen setzt das GIDS eine föderale Struktur voraus, bei der die Agenten und Sensoren in unabhängigen administrativen Domänen stehen. Das führt dazu, dass im GIDS weder ein direktes Vertrauensverhältnis zwischen den Agenten besteht, noch deren Funktion und Betrieb direkt dem GIDS Betreiber untersteht. Dies führt also dazu, dass die Architektur des Domino Systems nicht direkt für das GIDS übertragbar ist.

Im GIDS könnte das Problem durch eine stärkere Vernetung des Peer-2-Peer Netzwerkes gelöst werden, indem beispielsweise jeder GIDS Agent mit jeweils zwei anderen Agenten vernetzt ist. Vorteil ist, dass es keinen „Single Point of Failure“ gibt. Nachteile sind der administrative Aufwand zum Aufbau und der Pflege des Netzwerkes und dass die Ressourcenbetreiber Informationen über die Position ihres GIDS Agenten an andere Ressourcenbetreiber weitergeben müssen.

Für die Kommunikation zwischen den verteilten Agenten im GIDS könnte beispielsweise die Prelude Bibliothek in [6] eingesetzt werden. Vorteil dieser Bibliothek ist, dass sie die Anforderungen an den Datenschutz erfüllt, mit digitalen X.509-Zertifikaten umgehen kann und bereits das Format IDMEF unterstützt.

5.3 Repositories als alternativer Zugriff auf GIDS-relevante Daten und Informationen

In Kapitel 5.2 wurde ein dezentraler Ansatz der Datenverteilung diskutiert. Einen zentralistischen Ansatz kann man durch Repositories bieten. Dabei werden in einem zentralen Verzeichnis die Daten vorgehalten und können von dort aus an die Clients verteilt werden.

Da Repositories im Allgemeinen nur verwaltete Verzeichnisse zum Speichern von Daten sind, ist die tatsächliche technische Ausgestaltung sehr flexibel. Vor allem die Datenstruktur innerhalb eines Repositories ist keinesfalls festgelegt. Somit kann man sich vorstellen, die Datenbank, die beim GIDS-Betreiber liegt, als Repository einzurichten.

Das Befüllen eines Repositories ist auch sehr flexibel. Es bieten sich sowohl Push- als auch Pull-Mechanismen an. Im ersten Fall melden die GIDS-Agenten aktiv nötige Daten an das Repository. Das setzt jedoch voraus, dass die Agenten sich beim Repository authentifizieren und die Integrität der im Repository gespeicherten Daten gewährleistet ist. Zur Authentifikation kann wieder auf X.509-Zertifikate zurückgegriffen werden, die beim Aufbau einer sicheren Verbindung über die in Kapitel 5.1 beschriebene OpenVPN-Lösung genutzt werden. Bei Pull-Mechanismen hingegen geht die Aktion vom Repository aus. Dieses schickt eine Meldung per Broad- oder Multicast an die GIDS-Agenten. Diese wiederum antworten darauf und senden aktuelle Statusinformationen, die dann im Repository abgelegt werden.

Um ein Repository ausfallsicherer zu gestalten und auch um Überlastsituationen besser abfangen zu können, werden Repositories in der Regel auf mehrere physische Maschinen gespiegelt. Dabei ist es auch möglich, die Repository-Server bei verschiedenen Providern zu betreiben, so dass die Erreichbarkeit auch dann gewährleistet ist, wenn ein Provider komplett ausfällt. Jedoch bringt die Spiegelung von Daten einen großen Verwaltungaufwand mit sich, sofern sich die Daten häufig ändern. Gerade zeitkritische Daten, wie beispielsweise Warnmeldungen, müssen schnellstmöglich auf allen Spiegelservern vorhanden sein. Somit bietet es sich an, Repositories als Fallback-Lösung und für nicht zeitkritische Daten zu nutzen.

Ebenso wie das Befüllen der Daten, ist auch das Ausliefern neuer Daten sowohl durch Push- als auch durch Pull-Mechanismen möglich. In der Praxis werden jedoch vorwiegend Pull-Mechanismen eingesetzt, so dass die Clients eine Anfrage an den Server senden müssen, der seinerseits mit eventuell vorhandenen neuen Datensätzen antwortet.

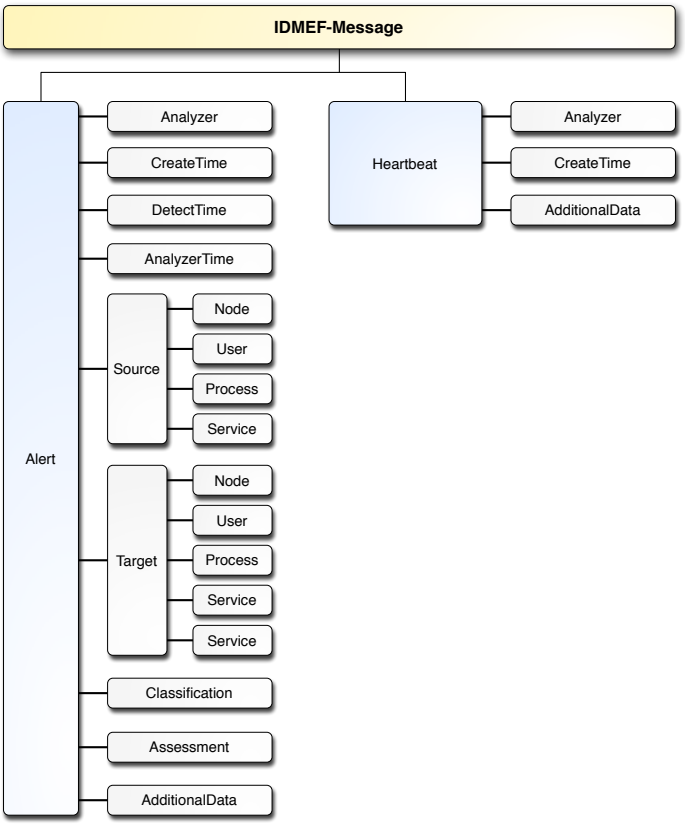


Abbildung 5.1: Das IDMEF-Datenmodell nach [5]

5.4 Datenaustauschformat IDMEF

Die *Intrusion Detection Working Group* (IDWG) der *Internet Engineering Task Force* (IETF) beschäftigt sich seit geraumer Zeit mit Datenformaten und Kommunikationsprotokollen zum Datenaustausch zwischen Komponenten von Intrusion Detection Systemen. Für diesen Prototypen fällt die Wahl auf das *Intrusion Detection Message Exchange Format* (IDMEF) nach [5].

5.4.1 Aufbau von IDMEF

Das IDMEF, das in Abbildung 5.1 illustriert wird, stellt ein einheitliches Nachrichtenformat für den Informationsaustausch zwischen Intrusion Detection Systemen dar. Ziel der Entwicklung eines solchen Formats ist die Flexibilität gegenüber verschiedenen Anwendungen. Dieser Anforderung trägt IDMEF durch eine Repräsentation der Nachrichten in der *Extensible Markup Language* (XML) Rechnung.

Ein großer Vorteil eines einheitlichen Nachrichtenformats ist die Möglichkeit zur Interoperabilität verschiedener Intrusion Detection Systeme. Anstatt herstellerspezifischer Kommunikationsmechanismen, die in der Regel nur eine Anbindung von Sicherheitskomponenten des gleichen Herstellers erlauben, bietet IDMEF eine Möglichkeit heterogene Sicherheitskonzepte zu realisieren.

Wie aus Abbildung 5.1 hervorgeht, existieren zwei Typen von IDMEF-Nachrichten. Es wird zwischen den sogenannten *Alert-* und den *Heartbeat-Nachrichten* differenziert.

Alert-Nachricht. Dieser Typ von Nachricht wird zur Meldung eines sicherheitsrelevanten Ereignisses versendet. Neben Informationen zum analysierten Element, welches die Meldung generiert hat, sind in einer Alert-Nachricht detaillierte Informationen zu Quelle

(*Source*) und Ziel (*Target*) des gemeldeten Ereignisses enthalten. Hierbei ist es insbesondere möglich, Angaben über IP-Adressen und Ports zu machen. Zusätzlich können die Nachrichten dieses Typs neben weiteren Details mit einer Reihe verschiedener Zeitstempel versehen werden, wie aus Abbildung 5.1 im linken Zweig der Illustration hervorgeht.

Heartbeat-Nachricht. Heartbeat-Nachrichten sind dazu gedacht, in regelmäßigen Zeitabständen von den einzelnen Komponenten eines gemeinsamen Systems verschickt zu werden. Diese Nachrichten signalisieren die Funktionsfähigkeit der jeweiligen Komponente. Ein Fehlen einer oder mehrerer Heartbeat-Nachrichten weist oftmals auf eine Funktionsstörung oder den Ausfall eines Teils des IDS hin, was wiederum ein Indiz für einen Angriff sein kann.

Zwar steht IDMEF oftmals in der Kritik, durch seine XML-Basis sehr Overhead-belastet zu sein, jedoch handelt es sich um ein standardisiertes Datenmodell, das unter anderem bereits von einigen Intrusion Detection Systemen erfolgreich eingesetzt wird. Vor allem liegen die Vorteile dieser Wahl in einer offenen und herstellerunabhängigen Spezifikation, zu der bereits einige Referenzimplementierungen existieren und somit eine Menge existierender Systeme problemlos in das GIDS integriert werden können.

5.4.2 IDMEF-Unterstützung von eingesetzten IDS-Lösungen

Voraussetzung für einen möglichen Einsatz von IDMEF im Rahmen des GIDS-Projektes ist die Kompatibilität zu bereits eingesetzten Produkten. Einige IDS-Produkte besitzen bereits nativ Funktionen, um entsprechende Daten im IDMEF zu liefern. Für andere gibt es zum Teil Adapter und Plugins, um sie IDMEF-fähig zu machen. Im Folgenden werden einige etablierte und zum Teil auch im D-Grid eingesetzte IDS hinsichtlich ihrer IDMEF-Unterstützung betrachtet.

Snort Snort ist ein signaturbasiertes Intrusion Detection System, das unter einer GPL-Lizenz (GNU General Public License) verfügbar ist. Für Snort sind viele IDMEF-Plugins als frei verfügbare Opensource-Lösungen vorhanden. Durch diese Plugins könnte Snort recht einfach in die GIDS-Infrastruktur eingebunden werden.

Prelude Beim Prelude Intrusion Detection System handelt es sich um ein sogenanntes hybrides IDS. Es ist nativ zu einer Vielzahl anderer IDS kompatibel. Die Bibliothek `libprelude` bietet einen verschlüsselten Transport und überprüft die Authentifizierung der Komponenten über X509-Zertifikate. Als nützliche Eigenschaft kann diese Bibliothek auch dafür verwendet werden, um aus Daten anderer Sensoren IDMEF-Nachrichten zu erzeugen. Die Bibliothek kann also auch innerhalb des GIDS verwendet werden, um andere Sensoren ohne nativen IDMEF-Export zu unterstützen. Weiterhin hat der Prelude Correlator im Rahmenwerk die Aufgabe, Alarme zu korrelieren und daraus aggregierte IDMEF-Nachrichten zu erzeugen.

Die Einbindung von Sensoren, ebenso wie die Nutzung verschiedenster Formate von Logdateien, zeichnen Prelude aus. In Bezug auf die Einbindung in die GIDS-Infrastruktur bietet das Prelude IDS ebenso eine native IDMEF-Unterstützung an. Mit Hilfe von Prelude könnte entsprechend auf eine Vielzahl verschiedener Sensoren zurückgegriffen und IDMEF Daten zwischen den verschiedenen GIDS-Beteiligten verschickt werden.

STAT STAT ist eine verteilte Umgebung für verschiedenartige IDS, die von der Universität California Santa Barbara entwickelt wurde. Ziel ist die zentraliserte Auswertung des momentanen Bedrohung auf der Basis der aggregierten und korrelierten Alarme, die sowohl von netzwerk-basierten als auch lokalen Sensoren erzeugt werden (siehe [13] und [12]). Als einheitliches Format wird unter anderem IDMEF unterstützt. Eine Implementierung ist als Opensource-Lösung vorhanden.

OSSEC Das lokale IDS OSSEC überprüft die Integrität des Betriebssystems und werte die System-Logs auf Angriffspuren aus. Zwar unterstützt das native OSSEC IDMEF noch nicht, allerdings sind bereits Erweiterungen vorhanden, die aber momentan noch nicht aus offiziellen Quellen stammen.

Cisco Cisco bietet mehrere Intrusion Detection und auch Intrusion Prevention Systeme. Die Firma Cisco hat sich aber für den mitentwickelten Industriestandard SDEE entschieden und dementsprechend keine Unterstützung von IDMEF vorgesehen.

Stonesoft In den IPS-Lösungen von Stonesoft ist es möglich, Log-Daten in verschiedensten Formaten zu exportieren ([10]). Es wird zwar offiziell kein IDMEF-Format angeboten, jedoch ist es möglich Daten im XML-Format zu erhalten. Diese können dann, wenn man den XML-Export nicht personalisieren kann, durch eine Transformation in das IDMEF-Format übertragen werden. Nativ unterstützt die Lösung von Stonesoft Suns Snoop-Format.

5.5 Grobübersicht eines Integrationskonzepts

Zur Unterstützung des föderierten IDS im D-Grid ist eine leichte und effiziente Integration der Partner wichtig. Neben der technischen Integration der Sensorik und der Installation der GIDS-Komponenten ist aber auch die Festlegung des organisatorischen Ablaufs wichtig. Grob umrissen sind insgesamt die folgenden Schritte von Bedeutung:

Registrierung Der erste Schritt der Integration von Partnern im D-Grid ist die Anmeldung und Registrierung bei dem Betreiber oder Betreiber-Konsortium des GIDS. Diese Daten sind beispielsweise bei administrativen Vorgängen notwendig und spielen eine wichtige Rolle bei der Warnung des Partners bei akuten Sicherheitsproblemen.

Kooperationsvereinbarung Die Kooperationsvereinbarung regelt die Zusammenarbeit zwischen dem Betreiber des GIDS und dem kooperierenden Partner. Sie ist insbesondere deshalb wichtig, weil alle am GIDS beteiligten Seiten ihre individuellen Bedürfnisse haben und ist spätenstens bei dem Start des produktiven oder kommerziellen Betriebs notwendig. So ist in vielen Fällen die Zusicherung des vertraulichen und sicheren Umgangs mit deren Daten eine notwendige Voraussetzung für die Teilnahme von Ressourcenanbietern. Weiterhin hat der Betreiber des GIDS das Interesse, dass vertrauliche Daten für den Betrieb des Systems nicht von Ditten an Unbefugte weitergegeben werden. Der wohldefinierte Umgang mit den Daten ist also für alle Seiten von Bedeutung. Der kommerzielle Betrieb des GIDS verlangt die Festlegung von Service Levels, die dann in der Kooperationsvereinbarung festgehalten werden können.

Technische Intergration Um möglichst viele Partner aus dem D-Grid für das GIDS zu gewinnen, ist eine leichte und effiziente Integration der GIDS-Komponenten Voraussetzung. Dies betrifft sowohl die Anbindung bereits vorhandener Sensoren als auch die Installation der GIDS-Komponenten einschließlich des GIDS-Agenten und der lokalen Datenspeicher.

Die technische Integration der GIDS-Komponenten kann auf verschiedenen Wegen erfolgen. Da für den GIDS-Agent und Datenspeicher exakt spezifizierte Schnittstellen und Austauschformate (beispielsweise IDMEF) vorgesehen sind, existieren keine direkten Abhängigkeiten zu den bereits vorhandenen Komponenten seitens der Ressourcenbetreibers. Deshalb können diese entweder als gekapselte Softwarepakete, Betriebssystem-Images oder im Extremfall als schlüsselfertige Appliance zur Verfügung gestellt werden. Es müssen dann nur noch die Schnittstellen zur Datenübertragung, die Anonymisierung bzw. Pseudonymisierung und der Datenexport angepasst werden. Das macht die Integration dieser Komponenten so einfach wie möglich. Desweiteren können auch fertig gekapselte Sensoren wie beispielsweise Snort auf diesen Wegen angeboten werden. Deren Integration ist dann ohne großen Aufwand möglich. Etwas schwieriger ist die Anbindung bereits bestehender Komponenten. Diese umfassen beispielsweise Grid-Systeme zum Auditing und bereits vorhandene IDS, die in das GIDS integriert werden sollen. Für bereits bekannte Systeme wie beispielsweise Snort können Software-Pakete zur Verfügung gestellt werden, die die Daten im IDMEF[1] versenden. Allerdings kann ein gewisser Aufwand zur manuellen Integration nicht verhindert werden. Allerdings bietet sich hier die Möglichkeit,

[1] Für Snort existiert beispielsweise ein Plug-in, das die Alarme als IDMEF-Nachrichten exportiert.

die Intergration von proprietären Komponenten im Rahmen des Verwertungsplans als Dienstleistung anzubieten.

Kapitel 6

Zusammenfassung & Ausblick

Ziel dieses Dokuments ist die Spezifizierung eines Grobentwurfs für das Grid-IDS (GIDS), der später die Basis für die weitere Verfeinerung bildet. Dies beinhaltet sowohl eine grundlegende Entscheidung für eine Architektur des IDS-Netzwerkes als auch für die organisatorischen und administrativen Aspekte, die beispielsweise durch die Rollen im GIDS wiedergegeben werden.

Grundlage für die Erstellung des Grobkonzeptes bilden die Anforderungen, die im dritten Kapitel wiederholt werden. Diese setzen sich aus den folgenden Anforderungen zusammen: Technische Anforderungen an die Erkennungsleistung, organisatorische und rechtliche Anforderungen, Anforderungen an die Sicherheit des Systems und weitere Anforderungen, die sich beispielsweise aus der Integration in das Grid-Umfeld ergeben. Eine der grundlegenden Anforderungen ist der föderale Charakter des GIDS, der eine weitgehende Unabhängigkeit der am GIDS beteiligten Seiten fordert. Diese sind der Betreiber des GIDS, die Ressourcenanbieter und weitere Rollen. Als Konsequenz des föderativen Charakters wurde eine Kapselung und die technische sowie administrative Unabhängigkeit dieser Seiten in der Architektur vorgestellt. Grundlegende Idee ist die Trennung in einen lokalen Bereich, in dem die Partner organisatorsich und administrativ unabhängig agieren könnnen. Dieser beinhaltet die technischen Sensoren bzw. Agenten zur Erkennung von Angriffen und eine lokale Analyseeinheit und Reporting-Komponente. Auf die letzten beiden Komponenten hat nur der entsprechende Partner direkten Zugriff. Weiterhin ist ein globaler Bereich vorgesehen, der den Export der Daten und eine globale Analyseeinheit und Reporting-Komponente beinhaltet. Konzeptionell sind die beiden Bereiche gleich aufgebaut, jedoch sind die Daten im globalen Bereich für jeden Partner zugreifbar.

Die Architektur selbst besteht, wie im dritten Kapitel beschrieben, aus unabhängigen Domänen der Ressourcenanbieter und dem Betreiber des GIDS. Die Domänen der Ressourcenanbieter sind in den im letzten Abschnitt beschriebenen globalen und lokalen Bereich geteilt. Technische Komponenten sind die lokale Datenspeicherung und Analyseeinheit, die Sensoren zur Aufzeichnung von Angriffen und der GIDS-Agent zur Aggregation, Filterung, Anonymisierung und dem Export der Daten. Der Transport der Daten zum GIDS-Betreiber erfolgt über eine Bus-Struktur. Weiterhin ist der Zugriff auf die Daten durch ein Benutzerportal vorgesehen. Für die Authentifizierung von Benutzern beim Portal ist eine Verbindung zu einem VO-Managementsystem geplant.

Neben den Rollen des Betreibers und der Ressourcenanbieter sind weitere Rollen vorgesehen. Insbesondere im produktiven Betrieb ist eine Kooperation mit Drittanbietern, Kunden und Analysten wichtig. Drittanbieter können Quellen von Angriffsinformationen sein, die beispielsweise Angriffs-Signaturen dem System beisteuern sowie CERTs[1] sein, die die GIDS-Daten für die Vorfallsbearbeitung verwenden. Weiterhin können die Daten durch Analysten ausgewertet und bewertet werden. Zwar kann diese Rolle auch von den Ressourcenanbietern oder dem GIDS-Betrereiber übernommen werden, jedoch ist auch eine Trennung der Rollen denkbar. Beispielsweise kann diese Rolle von externen Spezialisten (beispielsweise eines CERTs) übernommen werden, die entsprechendes Hintergrundwissen besitzen. Diese Rolle ist insbeson-

[1] CERT ist die Abkürzung für Computer Emergency Response Team und bezeichnet Teams, die unter anderem bei Sicherheitsvorfällen in Computernetzen Unterstützung leisten.

dere dann wichtig, wenn Dienstleistungen Kunden gegenüber erbracht werden. Beispielsweise ist es sinnvoll, dass eine VO als Kunde des GIDS auftritt, deren Daten von Analysten auf aktuelle Sicherheitsprobleme überwacht werden.

Im vierten Kapitel wurden Abhängigkeiten der Grobarchitektur zu anderen Arbeitspaketen bzw. anderen Komponenten des GIDS identifiziert und beschrieben. Hierbei stand zunächst das Informationsmodell zusammen mit dem Datenaustauschformat im Vordergrund. Die Grobarchitektur muss neben einer effizienten Datenübermittlung und -verarbeitung ebenso die Sicherheit der gesammelten und entstehenden Daten gewährleisten können. Hierzu zählt zum einen die sichere Datenhaltung und zum anderen die gesicherte (also verschlüsselte) Übertragung der Informationen zwischen den GIDS-Agenten. Auch das Datenformat, in dem die Informationen übertragen werden sollen, ist so zu wählen, dass sowohl die effiziente als auch die sichere Verarbeitung der Daten erfolgen kann. Ein weiterer Fokus wurde auf das Datenschutzkonzept gelegt. Während es beim Informationsmodell und einem entsprechenden Datenaustauschformat eher um technische Aspekte einer Realisierung ging beschäftigt sich das Datenschutzkonzept mit rechtlichen Aspekten und der Privatssphäre personenbezogener Daten. Das Prinzip des *Least Privilege* aus der Informationssicherheit stellt einen Grundbaustein für die Erarbeitung eines Datenschutzkonzepts dar. Regelungen über die Pseudonymisierung und Anonymisierung von Daten, ebenso wie eine sichere Authentifizierungs- und Autorisierungslösung sind im Rahmen des Datenschutzkonzepts zu erarbeiten. Neben der rechtlichen Konformität des Datenschutzkonzepts hinsichtlich der Erhebung von personenbezogenen Daten und deren Anlass und Verwendungszweck wurde ebenfalls auf die Bedürfnisse der an GIDS teilnehmenden Sites des D-Grids eingegangen.

Im vorangegangenen Kapitel wurden einige mögliche Implementierungsansätze dargestellt, die bei der Realisierung des GIDS-Projekts zum Einsatz kommen könnten. Die jeweiligen Lösungen wurden zunächst vorgestellt und im Anschluß kritisch hinsichtlich einer Verwendung in GIDS betrachtet. Die jeweiligen Vor- und Nachteile der einzelnen Lösungen wurden im Zuge dieser Betrachtung diskutiert. Geschützte Kommunikationswege sind ein wesentlicher Bestandteil des Gesamtprojekts. Daher wurde eine Realsisierung mittels des Opensource-Projekts OpenVPN in Betracht gezogen, weil es neben den Vorteilen der X.509-zertifikatsbasierten Authentifizierung, der Broad- und Multicast-Fähigkeit und dem Port-Sharing nur den lösbaren Nachteil eines zentralen Servers aufweist. Die Realisierung der Kommunikation zwischen den GIDS-Komponenten über ein Peer-to-Peer-Netzwerk wurde ebenfalls untersucht. Sie zeichnen sich vor allem durch ihre Robustheit gegenüber Ausfällen einzelner beteiligter Knoten aus. Das Domino System schien sich zunächst zur Implementierung der GIDS-Kommunikationsinfrastruktur zu eignen. Die Struktur des Domino Systems lässt sich aber nicht ohne weiteres auf das Gridszenario übertragen. Dies liegt zum einen an anderen Voraussetzungen bzgl. der Vertrauenswürdigkeit zwischen den Agenten und zum anderen am starken administrativen Aufwand, der zum Aufbau und zur Pflege eines solchen Netzwerks erforderlich wäre. Repositories als eine zentralisierte Lösung zur Verteilung von GIDS-Daten wurden im Abschnitt 5.3 beleuchtet. Sowohl durch Push- wie auch Pull-Mechanismen erlauben sie eine gesicherte Verteilung der Daten als Fallback-Lösung und für nicht zeitkritische Daten. Als letztes wurde als mögliches Datenaustauschformat IDMEF (Intrusion Detection Message Exchange Format) betrachtet. Das auf XML basierende und standardisierte Format wird kurz durch die Erläuterung der verschiedenen Nachrichtentypen vorgestellt und scheint sich sehr gut für einen Einsatz im GIDS-Projekt zu eignen.

Abbildungsverzeichnis

Literaturverzeichnis

[1] Ilija Basicevic, Miroslav Popovic, and Vladimir Kovacevic. Use of publisher-subscriber design pattern in infrastructure of distributed ids systems. In *ICNS '07: Proceedings of the Third International Conference on Networking and Services*, Washington, DC, USA, 2007. IEEE Computer Society.

[2] Till Dörges and Jürgen Sander. Integrating open source information — rumors & facts in early warning, January 2010.

[3] Erich Gamma, Richard Helm, Ralph Johnson, and John M. Vlissides. *Design Patterns: Elements of Reusable Object-Oriented Software*. Addison-Wesley Professional Computing Series, November 1994.

[4] 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.

[5] IETF. The intrusion detection message exchange format (idmef). *http://tools.ietf.org/html/rfc4765*, 2007.

[6] Prelude technologies. https://dev.prelude-technologies.com/.

[7] Helmut Reiser, Nils gentschen Felde, Felix von Eye, Jan Kohlrausch, and Christian Szongott. Anforderungs- und Kritierienkatalog (MS 6). Meilensteinbericht, D-Grid, January 2010.

[8] Michael Schiffers. *Management dynamischer Virtueller Organisationen in Grids*. Dissertation, Ludwig-Maximilians-Universität München, München, July 2007.

[9] Ben Stock, Jan Goebel, Markus Engelberth, Felix C. Freiling, and Thorsten Holz. Walowdac analysis of a peer-to-peer botnet. In *European Conference on Computer Network Defense*, Milan, Italy, 2009.

[10] Stonegate technical documentation — exporting and printing of fw/ips log records. `https://my.stonesoft.com/support/document.do?product=StoneGate&docid=2086`.

[11] OpenVPN Technologies. OpenVPN. `http://openvpn.net`.

[12] F. Valeur, G. Vigna, C.Kruegel, and R. Kemmerer. A Comprehensive Approach to Intrusion Detection Alert Correlation. *IEEE Transactions on Dependable and Secure Computing*, 1(3):146–169, July 2004.

[13] G. Vigna, F. Valeur, and R.A. Kemmerer. Designing and Implementing a Family of Intrusion Detection Systems. In *Proceedings of the European Software Engineering Conference and ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE 2003)*, pages 88–97, Helsinki, Finland, September 2003.

[14] Vinod Yegneswaran, Paul Barford, and Somesh Jha. Global intrusion detection in the domino overlay system. In *In Proceedings of Network and Distributed System Security Symposium (NDSS)*, 2004.