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

GIDS – Abschlussbericht

Bericht zum Abschluss des D-Grid Projekts GIDS

Autoren:

Dr. Wolfgang Hommel (Leibniz-Rechenzentrum)
Dr. Nils gentschen Felde (Ludwig-Maximilians-Universität München)
Felix von Eye (Leibniz-Rechenzentrum)

GEFÖRDERT VOM

Inhaltsverzeichnis

Kapitel 1

Kurzdarstellung des Vorhabens

1.1 Aufgabenstellung

Zur technischen Sicherung der Nachhaltigkeit einer deutschlandweiten Grid-Infrastruktur ist insbesondere der Bereich des Sicherheitsmanagements zu berücksichtigen. Bei den vor Projektbeginn im D-Grid existierenden Mechanismen gab es eine Lücke sowohl in der Überwachung der Infrastruktur auf Sicherheitsangriffe als auch im Sicherheits-Reporting. Die Aufgabenstellung dieses Projektes bestand darin, diese Lücken durch die Inbetriebnahme eines föderierten Intrusion Detection Systems in Grid-Umgebungen (GIDS) zu schließen.

Ziel dieses Projekts war die Bereitstellung eines GIDS-Dienstes für das D-Grid. Hierbei galt es, soweit wie möglich bestehende Ansätze zu integrieren und ein domänen- und organisationsübergreifendes Gesamtsystem zu entwickeln. Insbesondere die Fähigkeit, Virtuelle Organisationen (VO) zu unterstützen und diese auch als Kunden in Betracht zu ziehen, war 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 erkennen zu können, als dies mit unabhängigen und nur die lokale Sicht berücksichtigenden Sicherheitssystemen möglich ist. Somit kann durch ein Grid-weites IDS 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 ggf. 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 notwendig.

Nach der Entwicklung einer geeigneten Architektur für ein kooperatives und föderiertes IDS in Grid-Umgebungen stand die Implementierung und Produktivführung des Systems im Vordergrund. Nach Abschluss der Projektlaufzeit steht nun ein produktives Intrusion Detection System als Grid-Dienst im D-Grid zur Verfügung, das sowohl von Ressourcen-Anbietern als auch Kunden (VOs, Communities etc.) genutzt werden kann und durch das DFN-CERT betrieben wird.

1.2 Voraussetzungen, unter denen das Vorhaben durchgeführt wurde

1.2.1 Umfeld

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 einem vor allem sehr dynamischen Umfeld. Dieses ist unter verschiedenen Gesichtspunkten festzustellen, wie z. B. der hohen Dynamik verfügbarer Ressourcen oder auch der hoch dynamische Nutzergruppen bzw. Virtuellen Organisationen (VO). Zudem ergibt sich ein Grid-typisch heterogenes Umfeld, das sich sowohl in der Nutzerbasis als auch in den verwendeten und angebotenen IT-Systemen widerspiegelt. Auch existiert dies auf mehreren Ebenen und ist u. a. auch im Bereich der Ressourcen, der eingesetzten Grid-Middleware und auch bei eingesetzten Grid-Diensten zu beobachten. Nicht zuletzt sind die zum Teil bereits von den beteiligten Organisationen eingesetzten Sicherheitskomponenten und -werkzeuge zur Erkennung von Angriffen unterschiedlichster Art. Häufig ist keine Koppelung bestehender Komponenten möglich und der Grid-weite Austausch von Informationen bezüglich sicherheitsrelevanter Ereignisse wird nicht umgesetzt. Dies ist aber nicht nur auf die genannte Heteroge-

nität zurückzuführen, sondern auch auf Randbedingungen wie beispielsweise unterschiedliche Sicherheits- und Informationsverbreitungsrichtlinien („security and information sharing policies“) der beteiligten realen Organisationen. Darüber hinaus bieten Firewalls keinen ausreichenden 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.

Vor Projektstart existierte kein Gesamtkonzept für ein kooperatives, Grid-weit föderiertes Intrusion Detection System mit entsprechenden Reporting-Komponenten, das sich in ein Umfeld wie dem D-Grid einbetten ließ. Daher sollte ein Konzept für ein GIDS entwickelt und im D-Grid implementiert und in die Produktion überführt werden.

1.2.2 Beteiligte Partner

1.2.2.1 Leibniz-Rechenzentrum (LRZ)

Das Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften ist eines der drei nationalen Supercomputing-Zentren und zentraler IT-Dienstleister für die Münchner Hochschulen und Forschungseinrichtungen. Es betreibt mit dem Münchner Wissenschaftsnetz (MWN) eine leistungsfähige Kommunikationsinfrastruktur für rund 100.000 Endgeräte und über 120.000 Nutzern. Das LRZ ist an Forschungsprojekten auf den Gebieten des Sicherheitsmanagements, des Netz- und Systemmanagements, neuer Netztechnologien und des Grid-Computing beteiligt. Ein generisches Intrusion Prevention System – Secomat – realisiert ein statistisches und signaturbasiertes IPS, das zusätzlich über die Analyse des Kommunikationsverhaltens in der Lage ist, infizierte Systeme mit hoher Zuverlässigkeit zu erkennen und so den manuellen Bearbeitungsaufwand massiv zu reduzieren. Weiterhin hat das LRZ langjährige Erfahrung im Betrieb und der Entwicklung von Grid-Systemen und ist in zahlreiche nationale und internationale Grid-Projekte eingebunden (z. B. DGI-2, IVOM, D-MON, SLA4D-Grid, DEISA2, LCG/EGEE, PRACE). Im Rahmen von D-Grid und insbesondere DGI-2 mit Beteiligung u. a. an AAI/VO und IVOM sowie dem VO-Management im D-Grid ist bereits eine breite Vorkenntnis insbesondere im Bereich der IT-Sicherheit gewonnen worden. Mehrere wissenschaftliche Mitarbeiter des LRZ sind Mitglieder der Forschergruppe von Prof. Hegering und Prof. Kranzlmüller, die sich seit über 20 Jahren intensiv mit Netz- und Servicemanagement sowie des IT-Sicherheitsmanagements in komplexen, heterogenen, verteilten Umgebungen wie Grids, Clouds und Föderationen

befasst. In dieser Zeit entstanden mehr als 350 Veröffentlichungen, rund 50 Dissertationen und viele hundert Diplomarbeiten und Forschungsberichte.

1.2.2.2 Regionales Rechenzentrum für Niedersachsen (RRZN)

Das Regionale Rechenzentrum für Niedersachsen (RRZN) bietet als zentrale Einrichtung der Leibniz Universität Hannover (LUH) IT-Dienste und IT-Infrastruktur für Forschung, Lehre und Verwaltung an. Darüber hinaus versorgt das RRZN in regionalen und überregionalen Verbünden Hochschulen und Forschungseinrichtungen mit IT-Ressourcen und -Diensten. In einer seit 1996 bestehenden Kooperationsvereinbarung unterstützt das RRZN den Landesbetrieb für Statistik und Kommunikationstechnologie Niedersachsen (LSKN) bei Aufbau und Betrieb innovativer Technologien im Landesdatennetz Niedersachsen. Hierbei werden schwerpunktmäßig Fragestellungen zur Netzsicherheit bearbeitet, wie der Einsatz von Firewall-Lösungen oder Intrusion Detection/Prevention Systemen für Dienststellen und Ministerien des Landes Niedersachsens. Über die verschiedenen Fachgebiete des D-Grid Integrationsprojekts 2 (insbesondere FG-3 und FG-5), das gemeinsam mit FhG SCAI koordinierte IVOM Projekt, als Konsortialführer des Projekts GDI-Grid sowie als Ressourcenzentrum im D-Grid verfügt das RRZN über umfangreiche Erfahrungen in den Bereichen Entwicklung, Betrieb und Sicherheit von Grid-Systemen. Auf internationaler Ebene vertritt das RRZN die Interessen von D-Grid unter anderem in Arbeitsgruppen des Open Grid Forum (OGF) sowie als offizielle Delegierte in der e-Infrastructure Reflection Group (eIRG). Die Expertise des RRZN im Umfeld der IT-Sicherheit wird seit Jahren durch zahlreiche internationale Publikationen belegt. In den Forschungsthemen wird stets ein hoher Bezug zur Praxis gefordert, um die erarbeiteten Ergebnisse in Dienstleistungen des RRZN oder beteiligter Einrichtungen zu übertragen. Übergeordnetes Ziel ist es, die IT-Versorgung in Forschung, Lehre und Verwaltung unter technischen und wirtschaftlichen Aspekten hinsichtlich Stabilität, Sicherheit und Akzeptanz bei den Nutzern kontinuierlich voranzutreiben und zu verbessern.

1.2.2.3 DFN-CERT

Das DFN-CERT ist seit 1993 für einen sehr großen - und vor allem schnellen - Teil des deutschen Internets zuständig. Im Sinne einer zeitnahen Prävention erhalten die Anwender Informationen über neue Sicherheitslücken mit entsprechenden Abwehrmaßnahmen. Reaktiv wird Berichten oder Meldungen über konkrete Angriffe und Vorfälle nachgegangen. Dabei stammen solche Berichte aus drei verschiedenen Quellen: angegriffenen Einrichtungen selbst, die Opfer geworden sind; angegriffe-

nen Einrichtungen, die den Angriff erfolgreich abgewehrt haben; anderen CERTs, in deren Klientel Angriffe festgestellt wurden. Aufgrund der reaktiven Arbeit gibt es einen reichen Erfahrungsschatz innerhalb des Teams mit neuen Angriffswerkzeugen sowie mit der Interpretation und Auswertung von Log-Dateien oder anderen Hinweisen auf Angriffe und erfolgreich kompromittierten Systemen. Inzwischen hat sich aus einem universitär geprägten Forschungsprojekt ein Dienstleistungsunternehmen mit starkem Fokus auf IT-Technologien herausgebildet, das eine Vielzahl von Sicherheitsdienstleistungen realisiert und weiterentwickelt. Inzwischen arbeiten 25 Mitarbeiterinnen und Mitarbeiter in vier verschiedenen Bereichen: CERT (im eigentlichen Sinne des Wortes), PKI, IT-Services und Forschungsaufgaben. Das DFN-CERT ist ein Leistungsträger in der nationalen und internationalen CERT-Landschaft, und war z. B. mit dem BSI zusammen Initiator des deutschen CERT-Verbunds im August 2002. Das DFN-CERT ist seit seiner Gründung 1993 international in verschiedenen Arbeitsgruppen bei der Analyse von Sicherheitslücken und Vorfällen engagiert, in denen auch neue Anwendungen wie z. B. Grids diskutiert werden. Im Zuge von Projekten auf europäischer Ebene war das DFN-CERT beim Aufbau eines internationalen Sensornetzwerkes beteiligt und führt dies zusammen mit anderen Partnern weiter fort. Außerdem ist es Partner in dem EU-Projekt NoAH zur frühen Erkennung von Computer-Würmern. Des Weiteren ist das DFN-CERT Betreiber eines Testbeds für traditionelle IT-Frühwarnung in verteilten Netzen im Rahmen eines mehrjährigen BSI-Projekts „Frühe Warnung im deutschen Internet (CarmentiS)“. Im Rahmen von Penetrationstests gibt es umfangreiche Erfahrungen mit der Bewertung des Sicherheitsstatus von Organisationen anhand von Netzwerktests. Für die zeitnahe Information betroffener Organisationen wurde eine Portallösung entwickelt. Hierdurch gelang es, die Informationsflut heutiger Überwachungssysteme zu einer echten Dienstleistung umzuwandeln.

1.2.2.4 Assoziierte Partner

Stonesoft Germany GmbH Die Stonesoft Corporation ist ein innovativer Entwickler von Lösungen zur integrierten Netzwerksicherheit und zum unterbrechungsfreiem Betrieb. Stonesoft operiert weltweit und konzentriert sich auf Enterprise-Kunden, für die fortschrittlichste Sicherheitstechnik, permanente Verfügbarkeit und geringe Gesamtkosten verbunden mit bestem Preis-/Leistungsverhältnis und hohem ROI wichtig sind. Die StoneGate™ Security Plattform vereint Firewall, VPN, SSL VPN Gateway und Intrusion Prevention System, end-to-end Hochverfügbarkeit und preisgekröntes Load-Balancing zusammen mit einem gemeinsamen, zentralen Management zu ei-

ner Sicherheitslösung, die sich ideal für Unternehmen mit verzweigten Strukturen eignet.
Die Stonesoft Corporation wurde 1990 gegründet und hat ihre Zentrale in Helsinki, Finnland. Niederlassungen im deutschsprachigen Raum befinden sich in Frankfurt und München.

Fujitsu Technology Solutions GmbH Die Fujitsu Technology Solutions (FTS, ehemals Fujitsu Siemens Computers) ist der führende europäische IT-Infrastruktur Hersteller und zugleich Marktführer in Deutschland. Mit seinem strategischen Fokus auf innovativen Mobility und Dynamic Data Center Produkten, Services und Lösungen bietet das Unternehmen eine einzigartige Bandbreite an Produkten – vom Notebook über Desktops bis hin zu IT Infrastrukturlösungen und Services. FTS ist in allen Schlüsselmärkten Europas, Afrikas und des Nahen Ostens präsent, der Bereich Infrastruktur Services ist in etwa 170 Ländern weltweit tätig.

1.3 Planung und Ablauf des Vorhabens

Das Projekt hatte eine Laufzeit von 36 Monaten (01. Juli 2009 bis 30. Juni 2012). Es gliedert sich auf in die folgenden neun Arbeitspakete:

AP	**Titel**	**Leitung**	**Dauer**
AP 1	Bestandsaufnahme bestehender Sicherheitssysteme und -dienste im D-Grid	LRZ	8 PM
AP 2	*Anforderungs- und Bedrohungsanalyse*		
AP 2.1	Anwendungsfall-getriebene Anforderungsanalyse anhand des D-Grid Szenarios	LRZ	5,5 PM
AP 2.2	Bedrohungsanalyse	DFN-CERT	5,5 PM
AP 2.3	Abgleich des Anforderungs- und Kriterienkatalogs mit existierenden Lösungen	RRZN	3,5 PM
AP 3	Entwicklung eines Datenschutzkonzeptes für ein föderiertes GIDS	DFN-CERT	5,5 PM
AP 4	Entwicklung eines Informationsmodells inkl. Datenaustauschformats	DFN-CERT	13 PM
AP 5	*Entwicklung einer Architektur*		
AP 5.1	Grobskizze einer Architektur für ein Grid-basiertes IDS	LRZ	6 PM

AP 5.2	Detaillierung der Architektur auf Seiten der Ressourcen-Anbieter, inkl. (technischer) Durchsetzung des Datenschutzkonzeptes	LRZ	3 PM
AP 5.3	Detaillierung der Architektur auf Seiten eines GIDS-Betreibers zur Erbringung eines Grid-weiten IDS-Dienstes	DFN-CERT	4,5 PM
AP 5.4	Evaluation des Architekturvorschlags im Hinblick auf Anforderungs- und Kriterienkatalog	RRZN	4 PM
AP 6	*Umsetzung der entwickelten Architektur im D-Grid*		
AP 6.1	Implementierung und Realisierung ausgewählter Agenten	LRZ	11,5 PM
AP 6.2	Implementierung und Realisierung von Komponenten zur sicheren Kommunikation untereinander	DFN-CERT	8,5 PM
AP 6.3	Implementierung und Realisierung einer Angriffserkennung für das GIDS	LRZ	13 PM
AP 6.4	Implementierung und Realisierung einer Benutzeroberfläche	RRZN	12 PM
AP 7	Kalibrierung des GIDS in Bezug auf das D-Grid Umfeld	LRZ	12 PM
AP 8	Tragfähigkeitsnachweis / Tests der Leistungsfähigkeit	RRZN	11 PM
AP 9	Produktivführung des GIDS	LRZ	7,5 PM

Der zeitliche Ablauf des Vorhabens sowie die an den jeweiligen Arbeitspaketen beteiligten Projektpartner gehen aus dem in Abbildung 1.1 dargestellten Gantt-Chart hervor.

1.4 Wissenschaftlich-technischer Stand, an den angeknüpft wurde

In [2] wird der Einsatz einer graphenbasierten Meldungsstrukturanalyse in einem domänenübergreifend arbeitenden Intrusion Detection System beschrieben. In [3] hingegen wird in derselben Umgebung der Einfluss von Anonymisierungstechniken von Anomalieerkennungsverfahren auf die Leistungsfähigkeit des zum Einsatz kommenden IDS untersucht. Diese beiden Arbeiten sind allerdings nicht

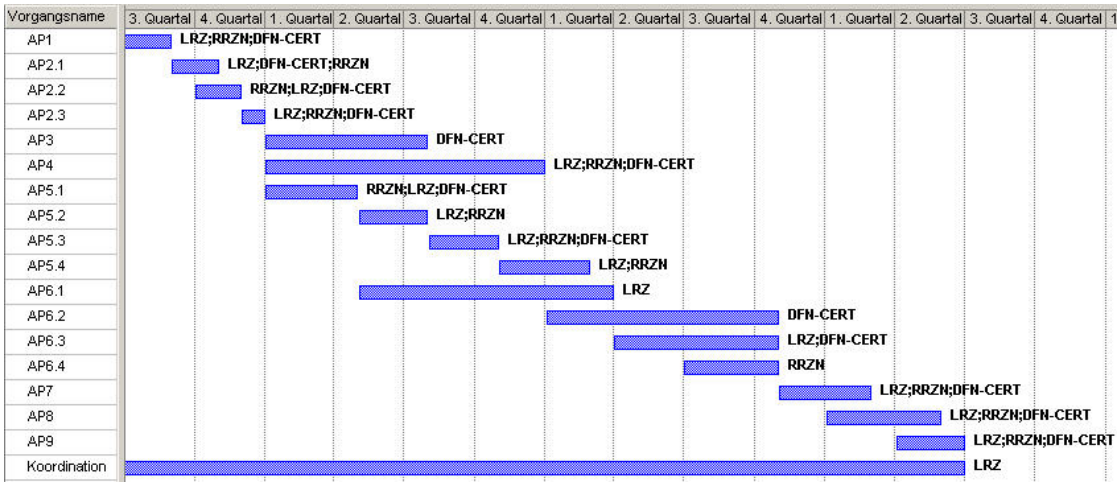

Abbildung 1.1: Zeitlicher Verlauf des Vorhabens

für den Einsatz im Grid geeignet. Insbesondere mangelt es ihnen noch an Grid-typischen Notwendigkeiten. Unter anderem fallen darunter z. B. Schnittstellen zu VO-Managementsystemen oder auch eine Untersuchung der Einsetzbarkeit in hochgradig dynamischen und vom Abstraktionsgrad höher liegenden Umgebungen (Stichwort: Virtualisierung von Diensten, Ressourcen, etc.).

Bereits 2003 ist in [1] das „Grid-based Intrusion Detection System“ vorgestellt worden. Erstmals wird der VO-Aspekt in einem Intrusion Detection System aufgebracht. Vielmehr noch wird das IDS selbst als eine VO modelliert. Nachteilig hingegen ist, dass eine Angriffsanalyse zentralisiert vorgenommen wird und seit 2003 eine Implementierung hierzu aussteht.

[27] und [28] präsentieren den Ansatz der „Grid Intrusion Detection Architecture“ (GIDA). Dabei 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 beiträgt. Allerdings setzt dieses System eine homogene Infrastruktur voraus, eine Erweiterung auf heterogene Umfelder fehlt. Außerdem führt eine Variation der Teilnehmerzahl am IDS zu einer enormen Rate an Fehlalarmen und sämtliche VO-Aspekte im Grid bleiben unberücksichtigt.

In einer aus dem Projekt „GridSec“ resultierenden Arbeit [16] wird eine Sicherheitsinfrastruktur vorgestellt, die Selbstverteidigungsmechanismen in Grid-Umgebungen zur Verfügung stellt. Diese Arbeit fokussiert maßgeblich auf die Erkennung aktiver Würmer und das Einleiten von Gegenmaßnahmen in Form von Verbindungsunterbrechungen. Somit deckt diese Arbeit nur einen sehr kleinen Aus-

schnitt der notwendigen Maßnahmen in Bezug auf IDS im Grid ab und lässt u. a. einen Mechanismus zur Berichterstattung (Reporting) erfolgreich erkannter Angriffe vermissen.

In den Arbeiten von Leu et. al. [18, 19] wird das „Performace-based Grid Intrusion Detection System“ (PGIDS) vorgestellt. Dabei werden die Grid-Knoten als Analyseeinheiten eingesetzt. Jede am IDS teilnehmende Partei erhält hierzu eine eigene, autonome Instanz des PGIDS, die durch einen zentralen Scheduler bedient wird. Die Nachteile dieses Systems sind vor allem, dass es durch den zentralen Scheduler einen Single-Point-of-Failure gibt und ein vollständiges Vertrauen zwischen den Teilnehmern voraussetzt. Zudem ist das System konstruktionsbedingt nur in der Lage netzbasierte Angriffe zu erkennen.

[26] und [25] schlagen eine Architektur für Grid-basierte IDS vor – das „Integrated Grid-based Intrusion Detection System“. Hierbei handelt es sich um ein übergeordnetes System, das eine Zusammenführung von Host- und Netz-basierten IDS vorsieht. Der Datenaustausch geschieht unter Nutzung des XML-basierten Intrusion Detection Message Exchange Format (IDMEF), alle Daten werden in Datenbanken im Grid abgelegt. Der Hauptnachteil dieses Konzeptes ist der zentralisierte Aufbau des Systems. Zusätzlich mangelt es dieser Architektur an einer Anbindung an VO Managementsysteme. Auch ein Mechanismus für das Reporting ist in dieser Architektur nicht bedacht und zurzeit sind keine konkreten Implementierungen verfügbar.

In [22] wird das „Self-adaptive Intrusion Detection System for Computational Grids“ präsentiert. Es basiert primär auf den von der GSI (Grid Security Infrastructure) bereitgestellten Diensten und bildet eine hierarchische Struktur von Agenten. Das Grid-basierte IDS wird anhand sogenannter Trust Communities 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 Modules (RM) auf einen erkannten Angriff reagieren. Nachteilig an diesem Ansatz ist, dass das Vertrauen unter den Trust Communities vorausgesetzt wird ohne Beachtung von Datenschutzrichtlinien oder Information-Sharing-Policies zu finden. Weiter sind VO-Aspekte im Sinne eines Kunden nicht weiter beachtet.

Im Rahmen des NextGRID-Projekts ist die Arbeit „Intrusion Detection and Tolerance in Grid-based Applications“ [32] entstanden. Im Rahmen der Arbeit wird eine generische Architektur für ein Grid-basiertes IDS präsentiert. Das Architekturkonzept lehnt sich an der Generic Monitoring Architecture (GMA) an und basiert auf dem darin eingesetzten Publisher-Subscriber-Prinzip. Für das Grid-

IDS relevante Daten werden durch Sensoren erfasst. Diese Sensoren sind alle in einem Verzeichnisdienst zentral erfasst und können darüber von einem Konsumenten abonniert werden. Im Falle des vorgestellten IDS handelt es sich bei dem Konsumenten um einen Korrelationsmechanismus, der die verfügbaren Sensordaten auf Angriffsszenarien unter Nutzung einer Korrelations-Datenbank hin untersucht. Eine Implementierung des Grid-basierten IDS existiert auf Basis diverser Web-Service Standards. Die größten Nachteile dieses Systems sind der Mangel an einem Datenschutzkonzept und die fehlende Möglichkeit, dieses technisch durchzusetzen. Im Rahmen dieses Projekt wird die auf Web-Services basierende Implementierung des Grid-IDS genauer untersucht werden und ggf. geeignete Teilkomponenten dieser Lösung mit in das für das D-Grid zu entwickelnde GIDS einfließen.

Zusammenfassend lässt sich festhalten, dass bereits eine Reihe an guten Ideen zur Lösung von kleineren Teilproblemen existiert. Es mangelt jedoch an einem umfassenden Gesamtkonzept für eine mögliche Lösung zum Einsatz im Grid-Umfeld.

1.5 Zusammenarbeit mit anderen Stellen

Die maßgeblichste Kooperation von GIDS besteht mit CarmentiS. Das Teilprojekt „Weiterentwicklung, Erprobung und Erforschung neuer Frühwarnmethoden – Zeitnahe Information und Alarmierung über neue Sicherheitslagen im deutschen Internet“ bildet einen Bestandteil des Projekts „Frühwarnung vor IT-Angriffen zum Schutz von Informationsinfrastrukturen“, das durch das BSI mit Mitteln des Zukunftsfonds der Bundesregierung realisiert wird.

Im Rahmen des Gesamtprojekts sollen die Grundlagen für die Entwicklung von IT-Frühwarnsystemen (IT-FWS) erforscht werden. Hierzu sollen mittels zu entwickelnder Sensoren und Auswertesystemen (Soft- und Hardware) IT-Angriffe wie beispielsweise Computerschadprogramme so früh wie möglich identifiziert werden, um Gegenmaßnahmen zu entwickeln und die Nutzer zu warnen.

Das DFN-CERT ist in dem Teilprojekt mit Forschungs-, Entwicklungs- und Betriebsaufgaben betraut. Ziel des Teilprojekts ist es, in Kenntnis der bisherigen Erfahrungen der Projektpartner durch konkrete Forschungs- und Entwicklungsvorhaben gezielt einzelne Bereiche anzugehen, um bisher fehlende oder noch nicht integrierbare Informationsquellen für eine möglichst frühe Warnung nutzbar zu machen.

Das Teilprojekt beruht auf der Feststellung, dass bisher effektive Verfahren fehlen, um die Informationen eines Lagebildes automatisiert für eine frühe Warnung zu nutzen. Hierzu fehlen zum einen Maßnahmen zur Ausweitung bereits

funktionierender Verfahren. Konkret bedeutet dies die teilautomatisierte Analyse von Malware (worunter jedwede Software mit bösartiger Funktionalität verstanden werden kann), die Integration erweiterter Verfahren zur Datengewinnung auf Systemebene und die Berücksichtigung der weiteren Entwicklung bei Standardsicherheitsmechanismen (insbesondere Verschlüsselungsverfahren in Netzwerkprotokollen). Zum anderen ist es unabdingbar, in die Analyse und Aggregation von vorliegenden Daten sowie die Synthese von Warnungen und Alarmen zu investieren. Ohne dies können die insgesamt zur Verfügung stehenden Daten nicht sachgerecht ausgewertet werden.

Besondere Bedeutung hat hierbei das vom DFN-CERT betriebene Testbed, das als integratives Instrument einen erheblichen Mehrwert schafft. Wie in anderen Forschungsvorhaben auch hat das Testbed einen anerkannten Nutzen in der praktischen Forschungs- und Entwicklungsphase, damit später die entwickelten Verfahren auch wirklich einsatzfähig sind. Durch die praxisnahen Einsatzbedingungen können frühzeitig Probleme bei der Skalierung, Wechselwirkung und Funktionsweise für alle beteiligten Rollen (Nutzer, Entscheider, Anbieter, Hersteller) identifiziert, bewertet und damit auch korrigiert werden.

Beitrag des Vorhabens Auf der einen Seite kann GIDS von dem Lagebild in CarmentiS profitieren. Das Lagebild gibt wichtige Bedrohungen wieder, die auch Grids betreffen. Weiterhin ist eine Korrelation mit Daten aus CarmentiS möglich. So kann potentiell bei einer Verbindung zu einem Grid-System überprüft werden, ob von diesem System andere Angriffe ausgegangen sind. Das ist beispielsweise bei einem Anmeldevorgang nützlich, bei dem unklar ist, ob gestohlene Passwörter oder Zertifikate ausgenutzt wurden.

Auf der anderen Seite kann CarmentiS von den Angriffsdaten des GIDS profitieren. Da die Daten von CarmentiS auch zur Warnung der betroffenen Seite durch das Incident Response Team (IRT) des DFN-CERTs verwendet werden, bietet sich das GIDS als weitere Datenquelle an.

Kapitel 2

Eingehende Darstellung des Vorhabens

2.1 Verwendung der Zuwendung und des erzielten Ergebnisses im Einzelnen, mit Gegenüberstellung der vorgegebenen Ziele

In diesem Abschnitt werden die Ergebnisse der einzelnen Arbeitspakete ausführlich dargestellt. Ebenso wird ein Vergleich mit den im Antrag des Vorhabens definierten Zielen der Arbeitspakete durchgeführt.

2.1.1 AP 1: Bestandsaufnahme bestehender Sicherheitssysteme und -dienste im D-Grid

2.1.1.1 Beteiligte Projektpartner

- Leibniz-Rechenzentrum (LRZ)
- Regionales Rechenzentrum für Niedersachsen (RRZN)
- DFN-CERT

Leitung: LRZ

Dauer: 8 PM

2.1.1.2 Erzielte Ergebnisse

In Arbeitspaket 1 wurde unter Zuhilfenahme eines Online-Fragebogen-Systems eine Umfrage zur Bestandsaufnahme durchgeführt. Ziel dieser Umfrage war, neben der Identifizierung der wesentlichen Anforderungen an ein föderiertes Intrusion Detection System im D-Grid, die Ermittlung des aktuellen Bestands im D-Grid.

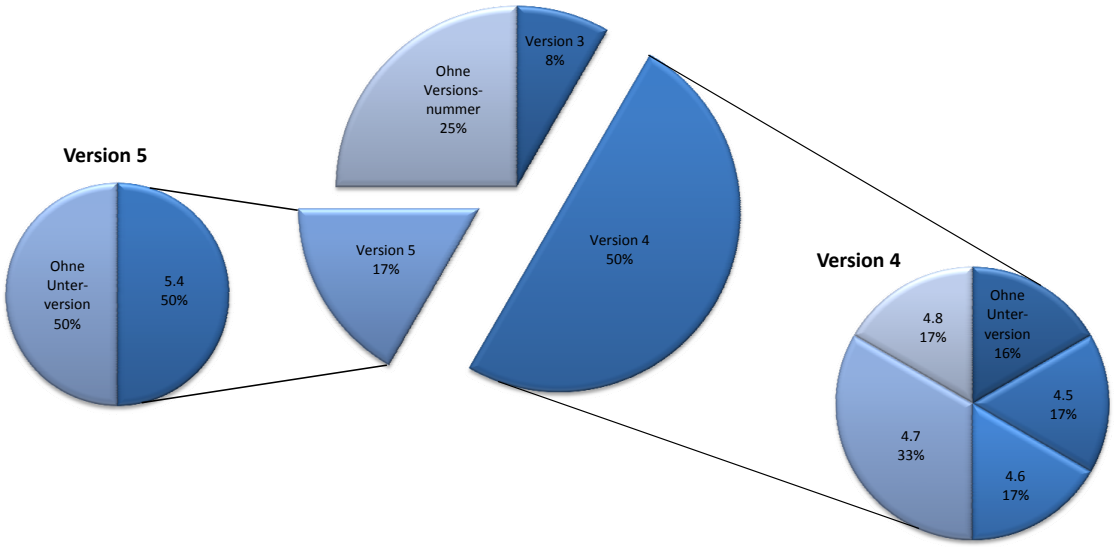

Abbildung 2.1: Ergebnis der Umfrage in Bezug auf die Versionsstände der eingesetzten Scientific Linux Distribution, aus [23]

In der durchgeführten Umfrage ist erwartungsgemäß ein sehr heterogenes Bild der D-Grid-Landschaft zu Tage getreten, das sich vor allem in der großen Vielfalt an Diensten, Betriebssystemen und Middlewares äußert. Die Abbildungen 2.1 und 2.2 zeigen exemplarisch einige Antworten auf den Fragebogen, die die Heterogenität in der eingesetzten Software zeigen. Speziell im Bereich Sicherheit wurde durch die Umfrage offenbart, dass eine große Differenz zwischen den einzelnen Ressourcenanbietern vorhanden ist. Auf der einen Seite bieten einige Provider 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 werden ebenfalls Ressourcen betrieben, bei denen keines der genannten Sicherheits-Tools eingesetzt wird und die sich einzig und alleine auf eine Firewall verlassen, die am Zugang vom X-Win zum Cluster installiert ist. Interessant ist das Teilergebnis der Umfrage, das bei etwa einem Drittel der Ressourcenanbieter in der Vergangenheit ein oder mehrere Sicherheitsvorfälle aufgetreten sind. Hierbei kann man von einer deutlich größeren Dunkelziffer ausgehen, vor allem bei den Providern, die keine Sicherheits-Tools auf den Grid-Knoten laufen lassen.

2.1.1.3 Gegenüberstellung mit den vorgegebenen Zielen

Ziel dieses Arbeitspakets war es, einen umfassenden Überblick über die im D-Grid eingesetzten Sicherheitssysteme zu erhalten. Neben einer reinen Bestandsaufnahme

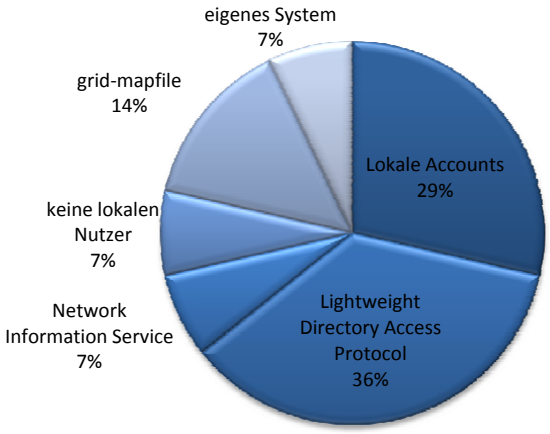

Abbildung 2.2: Ergebnis der Umfrage in Bezug auf die praktizierte Nutzerverwaltung, aus [23]

galt es, eingesetzte Systeme hinsichtlich ihrer Eignung für ein föderiertes Intrusion Detection zu untersuchen. Diese Ziele wurden allesamt erreicht. Eine Vielzahl von Systemen, die sich für eine Föderation eignen, wurden identifiziert und im späteren Gesamtsystem angebunden. Ebenso entstand im Laufe der Durchführung der Umfrage eine Liste von Ansprechpartnern, die bei den einzelnen D-Grid Sites für sicherheitsrelevante Fragen zur Verfügung stehen.

2.1.2 AP 2: Anforderungs- und Bedrohungsanalyse

Das Arbeitspaket 2 teilt sich in die Teilbereiche „Anwendungsfall-getriebene Anforderungsanalyse für IDS im D-Grid“ (AP 2.1), „Bedrohungsanalyse“ (AP 2.2) und „Abgleich des Anforderungs- und Kriterienkatalogs mit existierenden Lösungen“ (AP 2.3), die im Folgenden vorgestellt werden.

2.1.2.1 AP 2.1: Anwendungsfall-getriebene Anforderungsanalyse für IDS im D-Grid

Beteiligte Projektpartner

- Leibniz-Rechenzentrum (LRZ)
- Regionales Rechenzentrum für Niedersachsen (RRZN)
- DFN-CERT

Leitung: LRZ

Dauer: 5,5 PM

Erzielte Ergebnisse Um die Eignung eines Grid-basiertes IDS für den Einsatz im D-Grid bewerten zu können, wurde eine Reihe von Anforderungen definiert. Neben Anforderungen, die direkt aus der Auswertung der in Arbeitspaket 1 beschriebenen Umfrage folgerten, wurden weitere Anforderungen gefunden, indem verschiedene *Use Cases* betrachtet und aus diesen Anforderungen extrahiert wurden. Für diesen Zweck wurden verschiedene mögliche Anwendungsfälle untersucht und dabei herausgestellt, welche Akteure dabei beteiligt sind und welche speziellen Anforderungen diese an ein GIDS stellen könnten. Dabei wurde zwischen „Nutzergruppen- und Kundensicht auf ein GIDS“ und „informationsanbieter-spezifische Sicht auf ein GIDS“ unterschieden, da je nach Betrachtung unterschiedliche Anforderungen abgeleitet werden können. So ist beispielsweise der Ressourcenanbieter einmal Kunde gegenüber einer Betreiberrolle und einmal Informationsanbieter gegenüber einer Kundenrolle. Dies ist beispielsweise bei VOs der Fall, die berechtigt sind, die Grid-Ressourcen des Ressourcenproviders zu nutzen. In diesen Fällen unterscheiden sich die Anforderungen erheblich. Weiterhin wurden, um eine möglichst vollständige Auflistung aller Anforderungen zu erhalten, generische Anforderungen spezifiziert, die nicht speziell für ein Grid-basiertes IDS, sondern für Grid-Anwendungen allgemein gelten müssen zusammengetragen. Bei dieser Auflistung sind zwar einige Anforderungen auch schon in der obigen Anwendungsfall-getriebenen Anforderungsanalyse enthalten, jedoch wurden diese hier noch einmal aus einem anderen Blickwinkel betrachtet und gegebenenfalls ergänzt. Weiterhin wurden verschiedene Abstufungen von Kooperationsmustern und Vertrauensbeziehungen erläutert. Schlussendlich mündete die Auflistung in einer umfangreichen Tabelle, in der die einzelnen Anforderungen nach „funktionalen Anforderungen“, „nichtfunktionalen Anforderungen“, „Sicherheitsanforderungen“, „organisatorischen und Datenschutzanforderungen“ und „Anforderungen an die Erkennungsleistung“ angeordnet sind (siehe [23, Abschnitt 3.3]). Speziell die aus den Grid-Spezifika abgeleiteten Anforderungen, eine umfassende Unterstützung von VOs und deren Spezifika zu unterstützen, wurden konkretisiert.

2.1.2.2 AP 2.2: Bedrohungsanalyse

Beteiligte Projektpartner

- Leibniz-Rechenzentrum (LRZ)
- Regionales Rechenzentrum für Niedersachsen (RRZN)
- DFN-CERT

Leitung: DFN-CERT

Dauer: 5,5 PM

Erzielte Ergebnisse Bei der Bedrohungsanalyse wurden auf der einen Seite verschiedene Methoden vorgestellt, mit denen man sowohl technisch als auch analytisch Angriffserkennung betreiben kann. Auf der anderen Seite wird eine Analyse der aktuellen Bedrohungslage im Internet und bei Grid-Ressourcen durchgeführt. Anschließend sind Angriffe der Kategorien „Angriffe“, „Einsatz Malware auf Grid-Systemen“, „Missbrauch und Verletzung von Ressourcen“ und „Ausnutzung von Schwachstellen“ analysiert worden. Zu jeder Bedrohung werden neben einer einführenden Erklärung potentielle Abwehr- oder Erkennungsmechanismen aufgezeigt und eine erste Bewertung gegeben. Da für Grids keinerlei Statistiken über Angriffe vorliegen und sich im Allgemeinen der Schaden nur sehr schwer bemessen lässt, wird in diesem Rahmen bewusst auf eine quantitative Risikoabschätzung verzichtet. Die Analyse mündet in einen weiteren unabhängigen Anforderungskatalog. Dieser deckt sich jedoch in weiten Teilen mit dem Anforderungskatalog, der im Rahmen der Anwendungsfall-getriebenen Anforderungsanalyse in Kapitel 3.3 in [23] erstellt worden ist.

2.1.2.3 AP 2.3: Abgleich des Anforderungs- und Kriterienkatalogs mit existierenden Lösungen

Beteiligte Projektpartner

- Leibniz-Rechenzentrum (LRZ)
- Regionales Rechenzentrum für Niedersachsen (RRZN)
- DFN-CERT

Leitung: RRZN

Dauer: 3,5 PM

Erzielte Ergebnisse Bei der Untersuchung themenverwandter Arbeiten (vgl. Kapitel 1.4) wurden signifikante Defizite für die Eignung im D-Grid aufgezeigt, die einen Einsatz im D-Grid widersprechen. Dabei wurden viele verschiedenartige Ansätze mit unterschiedlichen Methoden zur Erkennung von Angriffen untersucht. Hauptkritikpunkt bei den meisten Ansätzen war, dass VO-Aspekte unberücksichtigt bleiben. Weiterhin wurden in den Arbeiten im Allgemeinen keine oder nur unzureichende Datenschutzaspekte berücksichtigt oder ein vollständiges Vertrauen aller beteiligten Partner wird vorausgesetzt. Schlussendlich wird in vielen Ansätzen nur ein Teil der Bedrohungsszenarien abgedeckt. Neben dieser eher

theoretischen Untersuchung wurden auch themenverwandte Implementierungen und Produkte untersucht. Dabei kam zu Tage, dass bis dato keine nativen Grid-IDS vorhanden waren, sondern dass verteilte IDS auf Grid-Strukturen abgebildet werden. Da diese aber eine Informationsanonymisierung designtechnisch nicht unterstützen, war der Datenschutz nicht gewährleistet.

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 3.3 in [23] erarbeiteten Anforderungen erfüllt. Die meisten eingesetzten Produkte bieten keine Grid-spezifische Unterstützung und können daher nicht ohne Erweiterungen die durch das Projekt geforderte föderierte Angriffserkennung in einem solch heterogenen Umfeld bieten.

2.1.2.4 Gegenüberstellung mit den vorgegebenen Zielen

Eines der Ziele dieses Arbeitspakets war es, die Angriffsziele und Risiken im Grid auf Basis der im D-Grid vorherrschenden Konzepte und Architekturen zu erarbeiten. Im Rahmen der durchgeführten Bedrohungsanalyse wurden sowohl Methoden erarbeitet, mit denen sowohl technisch als auch analytisch eine Angriffserkennung durchgeführt werden kann. Ebenso wurde eine Untersuchung zur derzeit aktuellen Bedrohungslage des Internets und von Grid-Ressourcen durchgeführt. Angriffe wurden kategorisiert und bewertet, um anschließend Angriffsmuster herausarbeiten zu können. Alle Aufgaben zur Erreichung dieser Ziele wurden erfolgreich durchgeführt und mündeten in einem Anforderungs- und Kriterienkatalog, der im Rahmen des Projekts als Meilenstein MS6 [23] veröffentlicht wurde.

Des Weiteren galt es, die Stärken und Schwächen bestehender Ansätze von Intrusion Detection Systemen für Grid-Infrastrukturen herauszuarbeiten und zu bewerten. Im Rahmen eines Abgleichs des Anforderungs- und Kriterienkatalogs mit existierenden Lösungen wurde das Fehlen geeigneter Systeme für Grid-Infrastukturen festgestellt. Die fehlenden Funktionalitäten existierender Lösungen wurden aufgedeckt und bezogen sich zu einem großen Teil auf Grid-spezifische Anforderungen, die es im Rahmen dieses Projekts zu entwickeln galt. Diese Defizite wurden in dem entwickelten Anforderungs- und Kriterienkatalog berücksichtigt, der als Basis für die weitere Entwicklung innerhalb des Vorhabens diente.

2.1.3 AP 3: Entwicklung eines Datenschutzkonzeptes für ein föderiertes GIDS

2.1.3.1 Beteiligte Projektpartner

- DFN-CERT

Leitung: DFN-CERT

Dauer: 5,5 PM

2.1.3.2 Erzielte Ergebnisse

Ziel dieses Arbeitspaketes war die Entwicklung eines Datenschutzkonzeptes, das alle rechtlichen, organisatorischen und technischen Anforderungen erfüllt, die vorher für das GIDS aufgestellt wurden. Weiterhin wird das Prinzip des „Least Privilege“ berücksichtigt, das die Berechtigungen und Möglichkeiten der beteiligten Sites auf das Notwendige einschränkt. Dadurch werden prophylaktisch die Risiken und Konsequenzen im Falle eines Sicherheitslecks so gering wie möglich gehalten. Das Arbeitspaket wurde mit einer Literaturrecherche bezüglich der vorhandenen Ansätze für Verfahren zur Anonymisierung und Pseudonymisierung personenbezogener Daten begonnen. Ziel war es, Komponenten zu bestimmen, die in das Datenschutzkonzept direkt oder mit minimalen Aufwand für Anpassungen übernommen werden können. So existiert beispielsweise mit „Crypto-PAn“ ein Rahmenwerk für die Pseudonymisierung von IP-Adressen. Als wichtiges Kriterium wurde geprüft, dass das Datenschutzkonzept konform zu den anderen Arbeitspaketen ist und deren Ergebnisse berücksichtigt. Das Ergebnis dieses Arbeitspaketes besteht aus einem Datenschutzkonzept ([10]), durch dessen Anwendung die geltenden Datenschutzgesetze eingehalten werden. Dieses Datenschutzkonzept diente im Folgenden in der praktischen Umsetzung als Vorlage.

2.1.3.3 Gegenüberstellung mit den vorgegebenen Zielen

Im Rahmen dieses Arbeitspakets ist gemäß dem Antrag ein Datenschutzkonzept entwickelt worden, welches alle anfallenden Anforderungen erfüllt. Technische und organisatorische Maßnahmen wurden untersucht und erarbeitet, um die in einem föderierten Intrusion Detection gesammelten Daten gemäß gesetzlicher Vorschriften und gemäß lokalen Sicherheitsrichtlinien zu behandeln. Eine wichtige Anforderung war, die Einhaltung des Datenschutzes in Einklang mit der Korrelation der Angriffsdaten des föderierten IDS zu bringen. Dabei wurde im ersten Schritt durch eine vollständige Anonymisierung der potentiell personenbezogenen Daten erreicht,

um die Einstiegshürde in das GIDS so niedrig wie möglich zu halten. Dadurch ist für den Betrieb des GIDS keine vertragliche Beziehung der Partner notwendig. Im zweiten Schritt ist vorgesehen, die Anonymisierung, soweit dies rechtlich möglich ist, zu vermeiden und beispielsweise durch eine Pseudonymisierung zu ersetzen. Eine rechtliche Grundlage dazu bietet die Übernahme der Kooperationsvereinbarung des CarmentiS Projektes, die optional von den GIDS-Partnern unterzeichnet werden kann. Die Policy für den Zugriff auf die Daten ist im Rahmen des Betriebsmodells veröffentlicht worden.

2.1.4 AP 4: Entwicklung eines Informationsmodells inkl. Datenaustauschformats

2.1.4.1 Beteiligte Projektpartner

- Leibniz-Rechenzentrum (LRZ)
- Regionales Rechenzentrum für Niedersachsen (RRZN)
- DFN-CERT

Leitung: DFN-CERT

Dauer: 13 PM

2.1.4.2 Erzielte Ergebnisse

Im Rahmen dieses Arbeitspaketes wurde die Spezifikation eines Informationsmodells inklusive eines Datenaustauschformats entwickelt. Für eine effiziente und zuverlässige Erkennung von Angriffen (insbesondere verteilter Angriffe über mehr als eine Site der D-Grid Infrastruktur) ist der sichere Austausch verschiedenartiger Daten zwischen den auf den Sites installierten GIDS-Komponenten erforderlich. Die Besonderheit dabei ist, dass die Kommunikation hier nicht nur Site-lokal, sondern ebenfalls Grid-global stattfindet. Im Rahmen des Arbeitspaketes wurde das Datenaustauschformat Intrusion Detection Message Exchange Format (IDMEF) als Grundbaustein für GIDS ausgewählt. Es hat sich gezeigt, dass IDMEF viele der Anforderungen an das GIDS-Datenformat erfüllt und vielfältige Erweiterungsmöglichkeiten besitzt, um es an die speziellen GIDS-Anforderungen anzupassen. Beispielsweise lässt sich IDMEF leicht für pseudonymisierte Daten erweitern. Alle anderen untersuchten Datenaustauschformate konnten entweder die Anforderungen nicht vollständig erfüllen oder waren als proprietäre Formate ungeeignet. Weiterhin handelt es sich bei IDMEF im Gegensatz zu vielen anderen proprietären Formaten um einen lebendigen Standard im Bereich verteilter IDS mit einer breiten

Nutzerschicht und einer aktiven Community. Aus diesen Gründen wurde IDMEF als Grundlage für das GIDS-Datenmodell ausgewählt. Dabei kann auf der bestehenden Syntax und Semantik aufgebaut werden. Die Erweiterungen ergeben sich aus den spezifischen Anforderungen des GIDS und führen schließlich zu dem GIDS-Datenmodell. Die Anpassungen an das GIDS-Datenaustauschformat betreffen die Spezifizierung einer eindeutigen Sensor-ID und die Aggregierung und Klassifizierung der IDMEF-Nachrichten. In verschiedenen Testinstallationen wurden diverse netz- und hostbasierte IDS auf ihre Kompatibilität mit IDMEF getestet. Dabei zeigt sich, dass die gewonnenen Daten die wichtigsten Anforderungen an das Austauschformat bereits erfüllen.

2.1.4.3 Gegenüberstellung mit den vorgegebenen Zielen

Ziel dieses Arbeitspakets war die Spezifikation eines Transportformats, um den sicheren und effizienten Transport der Daten von den Sensoren hin zu weiterverarbeitenden und analysierenden Komponenten des GIDS-Gesamtsystems sicherzustellen. Das Intrusion Detection Message Exchange Format (IDMEF) wurde als Basis für das Datenmodell und das Datenaustauschformat von GIDS festgelegt und an den für GIDS entscheidenden Stellen erweitert und angepasst. Somit steht nach Abschluss des Arbeitspakets sowohl ein Informationsmodell als auch ein Datenaustauschformat für die Verwendung innerhalb der GIDS-Infrastruktur bereit (siehe hierzu Meilenstein MS12 [12]).

2.1.5 AP 5: Entwicklung einer Architektur

Das Arbeitspaket 5 teilt sich in die Teilbereiche „Grobskizze einer Architektur für ein Grid-basiertes IDS“ (AP 5.1), „Detaillierung der Architektur auf Seiten der Ressourcen-Anbieter, inkl. (technischer) Durchsetzung des Datenschutzkonzepts“ (AP 5.2), „Detaillierung der Architektur auf Seiten eines GIDS-Betreibers zur Erbringung eines Grid-weiten IDS-Dienstes“ (AP 5.3) und „Evaluation des Architekturvorschlags im Hinblick auf Anforderungs- und Kriterienkatalog“ (AP 5.4), die im Folgenden vorgestellt werden.

2.1.5.1 AP 5.1: Grobskizze einer Architektur für ein Grid-basiertes IDS

Beteiligte Projektpartner

- Leibniz-Rechenzentrum (LRZ)
- Regionales Rechenzentrum für Niedersachsen (RRZN)

- DFN-CERT

Leitung: LRZ

Dauer: 6 PM

Erzielte Ergebnisse Für die Grobskizze der Architektur wurden zunächst die zentralen Rollen, unter denen Organisationen im Grid-Verbund auftreten können, und deren technische Komponenten für GIDS definiert. Für die Rolle *Ressourcenanbieter* sind Sensoren und die wichtigen Vorverarbeitungswerkzeuge *Filter*, *Aggregator/Verdichter* und *Anonymisierer / Pseudonymisierer* definiert. Daneben ist in der Architektur ein GIDS-Agent als Anbindung an eine Bus-Struktur vorgesehen, die eine Kommunikation zwischen den einzelnen Teilnehmern von GIDS ermöglicht, sowie eine optionale lokale (G)IDS-Instanz, die unabhängig von den anderen beteiligten Partnern Alarmmeldungen verarbeiten kann. Darüber hinaus werden jeweils Agentensysteme benötigt, die Meldungen von bestehenden bzw. zu schützenden und zu überwachenden Systemen erhalten und die diese Meldungen nach Durchlaufen der Vorverarbeitungsschritte an alle anderen für die jeweilige Nachricht relevanten GIDS-Partner verteilen können. Eine weitere zentrale Rolle ist der *Betreiber*, der in erster Linie für das Berichtswesen und die Anbindungen der Virtuellen Organisationen (VO) an GIDS über ein Benutzerportal bzw. für proaktive Benachrichtigungen zuständig ist. Weiterhin stellt er eine Grid-globale GIDS-Instanz und eine Datenbank für korrelierte Alarmmeldungen zur Verfügung. Als weitere Rollen wurden *Drittanbieter*, *Analysten* und *Kunden* spezifiziert. Die Rolle *Drittanbieter* beschreibt die Erweiterung um Informationen von Drittanbietern, aber auch um Integration von Informationsanbietern. Die Rolle *Analysten* spiegelt die Komplexität der Erkennung von Angriffen wider, da die Erkennung und das Reporting von Angriffen nur im begrenzten Umfang völlig automatisiert ablaufen kann. In der Rolle *Kunden* werden sowohl die teilnehmenden Ressourcenprovider als auch die VOs zusammengefasst, die über das Benutzerportal oder die proaktiven Benachrichtigungen des *Betreibers* Berichte und Alarmmeldungen einsehen können.

Im weiteren Verlauf wurden verschiedene Implementierungsmöglichkeiten für einzelne Komponenten untersucht und ihre Verwendbarkeit im Rahmen von GIDS bewertet. Schwerpunkte der Untersuchung waren zum einen das Datenaustauschformat und zum anderen die verschiedenen Möglichkeiten zur Realisierung einer geschützten Kommunikation für den Austausch von Daten. Dafür wurden verschiedene Kommunikationsansätze untersucht (Bus vs. Peer-to-Peer). Die Entscheidung

ist hierbei auf eine Bus-Architektur gefallen, die die gegebenen Anforderungen besser erfüllen kann als ein Peer-to-Peer-Ansatz. Kritsch ist im Peer-to-Peer-Ansatz die Entscheidung, wann alle Partner die Informationen erhalten haben und der Versand der Informationen abgebrochen werden kann. Weiterhin ist der administrative Aufwand größer, da die GIDS-Agenten bekannt sein müssen. Neben der Verbreitung sicherheitsrelevanter Informationen über den GIDS-Bus wurde ebenfalls eine Lösung über Repositories diskutiert, um als GIDS-Teilnehmer auf den aktuellen Datenbestand des Grid-basierten IDS zugreifen zu können. Auch die sichere und effiziente Übertragung von Angriffsdaten wurde beleuchtet. Weiterhin wurden mögliche Integrationskonzepte eruiert, um eine nahtlose Einbindung in die bei den beteiligten Organisationen typischerweise bereits vorhandenen IT-Infrastrukturen zu ermöglichen. Die entstandene Gesamtarchitektur ist in Abbildung 2.3 dargestellt.

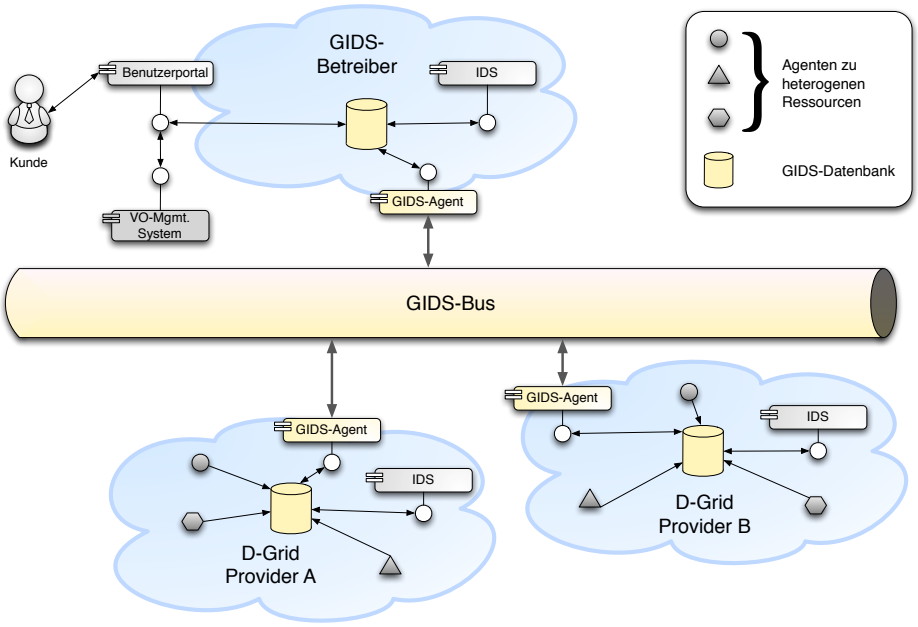

Abbildung 2.3: Überblick über die GIDS Infrastruktur

2.1.5.2 AP 5.2: Detaillierung der Architektur auf Seiten der Ressourcen-Anbieter, inkl. (technischer) Durchsetzung des Datenschutzkonzepts

Beteiligte Projektpartner

- Leibniz-Rechenzentrum (LRZ)

- Regionales Rechenzentrum für Niedersachsen (RRZN)

Leitung: LRZ

Dauer: 3 PM

Erzielte Ergebnisse Die in den vorherigen Arbeitspaketen definierten Komponenten und deren Funktionen wurden in diesem Arbeitspaket so detailliert spezifiziert, dass eine Implementierung auf dieser Basis erfolgen kann. Auf Basis der in Arbeitspaket 4 getroffenen Festlegung auf IDMEF und somit auf ein XML-basiertes Datenaustauschformat wurde hier untersucht wie die Vorverarbeiter *Filter*, *Aggregator / Verdichter* und *Anonymisierer / Pseudonymisierer* effizient implementiert werden können. Es wurde die Entscheidung getroffen, die Extensible Stylesheet Language (XSL) und XSL-Transformationen (XSLT) zu verwenden. Bei der Kommunikation über die GIDS-Bus-Struktur kann zur Reduktion des zu übertragenden Datenvolumens zudem auf Kompressionsmechanismen zurückgegriffen werden. Die eigentliche Logik des IDS liegt in den angeschlossenen (G)IDS-Instanzen. Die Installation und der Betrieb einer *lokale (G)IDS-Instanz* ist optional und dem jeweiligen Ressourcenanbieter eigenverantwortlich überlassen. Es bietet sich jedoch an, auf bereits existierende Mechanismen zurückzugreifen und diese an die Grid-Umgebung anzupassen. Die entsprechenden Vorüberlegungen für Betriebsmodelle und Integrationsstrategien wurden eruiert. Die Komponente *GIDS-Agent* ist die Komponente, die die Kommunikation, also den Informationsaustausch, zwischen allen teilnehmenden Sites realisiert. Sie bildete im Zusammenspiel mit den Implementierungsarbeiten in Arbeitspaket 6.1 einen der Schwerpunkte der Designaktivitäten.

2.1.5.3 AP 5.3: Detaillierung der Architektur auf Seiten eines GIDS-Betreibers zur Erbringung eines Grid-weiten IDS-Dienstes

Beteiligte Projektpartner

- Leibniz-Rechenzentrum (LRZ)
- Regionales Rechenzentrum für Niedersachsen (RRZN)
- DFN-CERT

Leitung: DFN-CERT

Dauer: 4,5 PM

Erzielte Ergebnisse Analog zu Arbeitspaket 5.2 werden in Arbeitspaket 5.3 die in Arbeitspaket 5.1 definierten Komponenten und deren Funktionen so detailliert spezifiziert, dass eine Implementierung auf dieser Basis erfolgen kann. Die dabei definierte Komponente *Benutzerportal* dient in erster Instanz dazu, kundenspezifische Sichten auf die verfügbaren Reports zu realisieren. Alle in diesem Portal verfügbaren Informationen sind durch ihre zuvor datenschutzkonforme Aufarbeitung prinzipiell für alle Anwender im Grid einsehbar. Es wird jedoch zusätzlich eine Sicht auf die Berichte angeboten, die nur die eigenen Ressourcen bzw. die von einer VO verwendeten Ressourcen umfasst. Analog zu Arbeitspaket 5.2 liegt die eigentliche Logik des IDS wieder in der angeschlossenen *Grid-globalen IDS-Instanz*. Die beim Betreiber des GIDS zum Einsatz kommende Grid-globale IDS-Instanz ist im Wesentlichen technisch identisch mit den lokalen (G)IDS-Instanzen auf Ressourcenanbieterseite. Aufgrund von Filterung und Anonymisierung der Daten muss jedoch mit einem weniger präzisen Datenbestand gerechnet werden, zudem die lokalen Auswertungen zusätzlich zu den GIDS-global verfügbaren auch die eigenen ungefilterten Daten zur Analyse heranziehen können. Für eine *proaktive Benachrichtigung* der Kunden des Grid-basierten IDS ist eine mandantenfähige Komponente notwendig, mit deren Hilfe Benachrichtigungen über einen erkannten Sicherheitsvorfall abhängig von seinem Schweregrad über verschiedene Kommunikationswege, wie beispielsweise E-Mail oder SMS, versendet werden. Um eine proaktive Benachrichtigungskomponente zu realisieren, wurden Konzepte zum Einsatz bzw. zur Modifikation bereits existierender Monitoring-Systeme diskutiert.

2.1.5.4 AP 5.4: Evaluation des Architekturvorschlags im Hinblick auf Anforderungs- und Kriterienkatalog

Beteiligte Projektpartner

- Leibniz-Rechenzentrum (LRZ)
- Regionales Rechenzentrum für Niedersachsen (RRZN)

Leitung: RRZN

Dauer: 4 PM

Erzielte Ergebnisse Eine umfassende Bewertung des Architekturvorschlags im Hinblick auf Anforderungs- und Kriterienkatalog [23] wurde durchgeführt. Dabei hat sich herausgestellt, dass die entwickelte Architektur den Anforderungs- und Kriterienkatalog weitestgehend erfüllt. Bei einigen Kriterien hat sich jedoch herausgestellt, dass eine umfassende Bewertung ohne die konkrete Implementierung

noch nicht möglich war. Hierzu gehörte insbesondere die nahtlose Integration in schon vorhandene Managementwerkzeuge. Weiterhin war für eine endgültige Bewertung die vollständige praktische Implementierung des Datenschutzkonzepts [10] nötig. Dafür wurde innerhalb von Arbeitspaket 6.2 ein technischer Leitfaden zur Umsetzung des Datenschutzkonzeptes erstellt. Die Umsetzung der noch offenen Punkte, die erst durch ihre konkrete Implementierung bewertet werden können, wurden in der weiteren Entwicklung des Vorhabens addressiert.

2.1.5.5 Gegenüberstellung mit den vorgegebenen Zielen

Im Rahmen dieses Arbeitspakets sollte eine Architektur für das föderierte Intrusion Detection System entwickelt werden. Diese Architektur muss verschiedenen Anforderungen genügen, wie beispielsweise der Wahrung der Autonomie aller an GIDS beteiligten Parteien. Neben der Entwicklung einer Grobarchitektur des Gesamtsystems standen ebenfalls Verfeinerungen sowohl auf Seiten der Ressourcenanbieter als auch auf Seiten des GIDS-Betreibers im Mittelpunkt dieses Arbeitspakets. Abschließend sollten die im Rahmen dieses Arbeitspakets entwickelten Architekturvorschläge mit dem Anforderungs- und Kriterienkatalog abgeglichen und bewertet werden.

Bei der Entwicklung der Gesamtarchitektur wurden zunächst alle an GIDS beteiligten Rollen und ihre Aufgaben festgehalten. Des Weiteren sind Abläufe und Vorgehensweisen definiert worden, wie sich Alarmmeldungen innerhalb des Systems bewegen und GIDS-weit veröffentlicht werden können, ohne dass hierbei personengebundene Daten, die datenschutzrechtlich geschützt werden müssen, weitergegeben werden.

Der Entwicklung der einzelnen Komponenten ging im Rahmen dieses Arbeitspakets eine genaue Untersuchung verschiedener Lösungsmöglichkeiten voraus. Verschiedene technische Lösungen wurden ermittelt, untersucht und auf ihre Verwendbarkeit innerhalb der GIDS-Infrastruktur bewertet. Neben Komponenten, die der Gesamtinfrastruktur dienen, wurden verfeinernd ebenso mögliche Implementierungsansätze für Komponenten auf Seiten der Ressourcenbetreiber als auch auf Seiten des GIDS-Betreibers untersucht.

Nach Abschluss des Arbeitspakets standen gemäß dem Antrag alle für die weiteren Arbeiten notwendigen Architekturkonzepte zur Verfügung und wurden in den Meilensteinen MS10 und MS16-1 [9, 11] veröffentlicht.

2.1.6 AP 6: Umsetzung der entwickelten Architektur im D-Grid

Das Arbeitspaket 6 teilt sich in die Teilbereiche „Implementierung und Realisierung ausgewählter Agenten“ (AP 6.1), „Implementierung und Realisierung von Komponenten zur sicheren Kommunikation untereinander“ (AP 6.2), „Implementierung und Realisierung einer Angriffserkennung für das GIDS“ (AP 6.3) und „Implementierung und Realisierung einer Benutzeroberfläche“ (AP 6.4), die im Folgenden vorgestellt werden.

2.1.6.1 AP 6.1: Implementierung und Realisierung ausgewählter Agenten

Beteiligte Projektpartner

- Leibniz-Rechenzentrum (LRZ)

Leitung: LRZ

Dauer: 11,5 PM

Erzielte Ergebnisse Aufgrund der Komplexität der Architektur ist es für deren technische Realisierung notwendig, auf bestehenden Systemen aufzubauen. Dabei müssen die bereits getroffenen Entscheidungen bzgl. der Grobarchitektur und des Datenschutzkonzeptes berücksichtigt werden. Als Basis für die Entwicklung eigener Agenten hat sich das Prelude-Framework angeboten, das die grundlegenden Funktionalitäten eines verteilten IDS mit offenen Schnittstellen enthält und durch seine Eigenschaft als Open-Source-Projekt anpassbar ist. Als weiterer Vorteil wird das Format IDMEF bereits nativ unterstützt und es bietet ein Datenbankschema, in dem Daten gespeichert werden können.

An dieses Framework wurden eine Reihe von Sensoriken unterschiedlichen Typs angebunden, wie beispielsweise Snort (Netz-basiertes IDS), OSSEC (Host-basiertes IDS) oder Prelude LML (Logfile Analyzer). Es ist jedoch wie bei AP 6.3 beschrieben eine weitere Verarbeitung der Sensor-Daten zur Reduzierung der False-Positives und zur Korrelation bzw. Aggregation erforderlich.

2.1.6.2 AP 6.2: Implementierung und Realisierung von Komponenten zur sicheren Kommunikation untereinander

Beteiligte Projektpartner

- DFN-CERT

Leitung: DFN-CERT

Dauer: 8,5 PM

Erzielte Ergebnisse Ziel des Arbeitspakets ist die Realisierung von Komponenten zur sicheren Kommunikation untereinander. Diese beinhalten die Realisierung der Datenspeicher und zugehörigen Schnittstellen zum Im- und Export der Daten. Dabei müssen diese Komponenten sowohl die vorher definierten Sicherheitsaspekte Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit gewährleisten, als auch sich in das Informationsmodell eingliedern.

Für die GIDS-Architektur bedeutet dies, dass die Daten sowohl sicher beim Ressourcenprovider erhoben als auch durch die GIDS-Infrastruktur übertragen werden müssen. Dabei müssen an allen Stellen die Datenschutzaspekte berücksichtigt werden. Die Umsetzung der ersten zwei Aspekte erfolgte durch Verwendung des Prelude-Frameworks und der OpenVPN-Software zum Transport der Daten für die GIDS-Architektur. Alle Komponenten wie beispielsweise IDS-Sensoren oder die VPN-Endpunkte werden durch X.509-Zertifikate authentifiziert und die Daten werden über verschlüsselte Kanäle versendet. In erfolgreichen Test der so implementierten Umgebung wurde sichergestellt, dass sowohl die im Anforderungs- und Kriterienkatalog aufgestellten Sicherheitsanforderungen erfüllt sind als auch die übrigen Anforderungen an die Leistungsfähigkeit nicht verletzt werden.

Zur Einhaltung des Schutzes personenbezogener Daten im Rahmen des Bundesdatenschutzgesetzes (BDGS) wurde das GIDS-Datenschutzkonzept, das insbesondere die juristischen Aspekte detailliert darstellt, auf das IDMEF-Datenformat bzw. alle von diesem vorgesehenen Attribute pro Sicherheitsereignismeldung angewandt. Somit liegt eine Beurteilung vor, in welchen Bereichen und in welchem Umfang ggf. personenbezogene Daten übertragen werden würden bzw. anonymisiert werden müssen. Dabei wurden Methoden zur Anonymisierung, vollständigen Filterung und Pseudonymisierung entwickelt und auf dem GIDS-Agenten eingesetzt, so dass diese in den Im- und Exportvorgängen der IDS-Nachrichten verfügbar ist.

Schlussendlich wurde im Zusammenspiel mit der Entwicklung des GIDS-Portals ein Rollenmodell entwickelt, das den sicheren Zugriff auf die IDS-Daten ermöglicht, und dieses in die Portalentwicklung integriert. Dabei wird für jede Rolle festgelegt, auf welche Daten diese Zugriff erhält. In diesem Rahmen können Ressourcenprovider dynamisch den Zugriff auf eigene Daten für virtuelle Organisationen beschränken. Technisch wurde diese Zugriffsbeschränkung im Portal realisiert.

2.1.6.3 AP 6.3: Implementierung und Realisierung einer Angriffserkennung für das GIDS

Beteiligte Projektpartner

- Leibniz-Rechenzentrum (LRZ)
- DFN-CERT

Leitung: LRZ

Dauer: 13 PM

Erzielte Ergebnisse Die Erkennung und Meldung lokaler Sicherheitsvorfälle oder von Daten, die eine Erkennung von Sicherheitsvorfällen ermöglichen, ist im Verantwortungsbereich der einzelnen Ressourcenprovider, die auch den Betrieb dieser Komponenten zu verantworten haben. Im Rahmen des Arbeitspaketes wurden, um die lokalen Meldungen zu simulieren und auch um den Ressourcenprovidern bei Bedarf funktionierende Lösungen anbieten zu können, mehrere Sensoriken betrieben. Darunter fielen neben den schon in AP 6.1 erwähnten Sensoren beispielsweise Simple Event Correlator (SEC) als Alternative zum Prelude Correlator oder Samhain (File Integrity Checker). Daher lag die Hauptaufgabe dieses Arbeitspaketes auf der Entwicklung einer für GIDS angepassten Korrelation der Alarme, um False-Positive-Meldungen der Ressourcenprovider zu minimieren. Für diesen Zweck wird der in das Prelude-Framework integrierte „Prelude-Correlator“ eingesetzt. Da dieser nicht für den Einsatz in einem Grid-IDS konzipiert wurde, mussten komplett neue Regelsätze entwickelt werden. Ferner wurden diese Regelsätzen an die technische Umsetzung der im Datenschutzkonzept geforderten Randbedingungen angepasst.

2.1.6.4 AP 6.4: Implementierung und Realisierung einer Benutzeroberfläche

Beteiligte Projektpartner

- Regionales Rechenzentrum für Niedersachsen (RRZN)

Leitung: RRZN

Dauer: 12 PM

Erzielte Ergebnisse Ziel dieses Arbeitspaketes ist die Entwicklung einer Benutzeroberfläche, die sowohl Gridbenutzern als auch Administratoren als zentrale Anlaufstelle für das GIDS dienen soll. Der leichte Zugang zum Portal und somit zu den zum Benutzer gehörenden sicherheitskritischen Daten ist eine wichtige Anforderung innerhalb dieses Arbeitspakets. Gridbenutzern soll im GIDS-Portal die Möglichkeit gegeben werden, sich über den aktuellen Sicherheitszustand der Ressourcen zu informieren, die sie zur Berechnung ihrer Jobs benutzen. Dies soll ohne weiteren organisatorischen Mehraufwand, wie beispielsweise die Beantragung eines neuen Zertifikats oder Passworts, möglich sein, weswegen auf die X.509-Zertifikate der Gridbenutzer zurückgegriffen wurde. Jeder aktive Gridbenutzer ist ohnehin bereits im Besitz eines solchen Zertifikats. Entsprechend erfolgt sowohl die Authentifizierung als auch die Autorisierung durch dieses Zertifikat. In beiden Fällen ist es möglich, sich entweder mit einem langlebigen Zertifikat oder mit Short Lived Credentials zu authentifizieren und autorisieren.

Speziell für die Anforderungen des Portals wurden einige Anpassungen der bestehenden Datenbanken nötig. Zum einen wurde, um die Anzeige von Alarmmeldungen im Portal zu beschleunigen, ein vereinfachtes, minimiertes Datenbankschema für IDMEF entwickelt. Eine von der eigentlichen Angriffserkennung unabhängige Datenbank hält so nur die Daten vor, die auch im Portal zur Anzeige genutzt werden sollen. Neben der Minimierung der Datenmengen und der Vereinfachung des Datenmodells wurden auch Erweiterungen der Datensätze beispielsweise für eine performante Autorisierung hinzugefügt. Weiterhin wird die Grid Resource Registration Service Datenbank (GRRS) einmal täglich gespiegelt und um nötige Felder erweitert. Alle Änderungen an der original GRRS-Datenbank sind entsprechend nach spätestens 24 Stunden auch für GIDS nutzbar.

2.1.6.5 Gegenüberstellung mit den vorgegebenen Zielen

Ziel dieses Arbeitspaketes war die technische Realisierung der Komponenten des föderierten GIDS auf Basis der Spezifikationen, die in den vorherigen Arbeitspaketen entwickelt worden sind. Dies betrifft sowohl die Sensorik als auch die anderen Komponenten des Systems: Implementierung der Schnittstellen, der Benutzeroberfläche, der Transportkanäle und der Datenspeicherung. Grundlage dafür ist die Spezifikation der Komponenten auf der Basis der vorherigen Arbeitspakete.

Speziell im Bereich der Sensorik sollten Agenten implementiert werden, deren Auswahl dabei maßgeblich auf den in AP1 ermittelten bereits bestehenden Sicherheitskomponenten sowie den drei im D-Grid eingesetzten Middleware-Konzepten Globus Toolkit, Unicore und gLite basieren sollte. Dies wurde dahingehend er-

reicht, dass durch die Wahl des Prelude-Frameworks bereits eine Vielzahl der bestehenden Sensoriken nativ unterstützt werden. Es wurden weiterhin Importroutinen implementiert, die ermöglichen, nicht unterstützte Sensoriken an das GIDS anzubinden. Somit werden alle in der Umfrage genannten Sensoriken unterstützt (vgl. dazu AP 1).

Im Teilbereich, der die Realisierung von Komponenten zur sicheren Kommunikation untereinander zum Thema hat, war das Ziel, einen Datenspeicher und Schnittstellen zu realisieren, die die Sicherheitsaspekte Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit gewährleisten. Dieses Ziel wurde dadurch erreicht, dass sowohl beim Design als auch bei der Implementierung der Kommunikationskomponenten auf eine sichere Verschlüsselung und auf die konsequente Nutzung von X.509 Zertifikaten geachtet wurde. Weiterhin wurde das Datenschutzkonzept vollständig umgesetzt, so dass alle relevanten Datenschutzaspekte berücksichtigt werden.

Die Zielsetzung im Teilbereich der Realisierung einer Angriffserkennung war die Untersuchung, ob und wie existierenden Ansätze zur Angriffserkennung herkömmlicher IDS eingesetzt werden können. Der verwendete Prelude-Correlator wurde im Rahmen des Arbeitspaketes auf seine Tauglichkeit geprüft. Dabei ist aufgefallen, dass dieser vom technischen Standpunkt aus gesehen für die Anforderungen von GIDS ausreichend ist, jedoch die vorhandenen Regelsätze innerhalb des Projektes unbrauchbar sind. Durch die Neuerstellung von einigen Regelsätzen konnte eine gute Erkennungsleistung erzielt werden.

Schlussendlich war im Teilbereich der Benutzeroberfläche das Ziel, eine integrierte Kommandozeilen- und Web-basierte Benutzeroberfläche zu erstellen, die sowohl für die zentrale Betriebsstelle als auch für die Ressourcenprovider und die Communities zur Verfügung steht. Dieses Ziel wurde ebenfalls vollständig erfüllt. Auf Seiten der Ressourcenprovider ist eine konsolenbasierte Konfigurationsmöglichkeit geschaffen worden und für die Nutzer der virtuellen Organisationen mit dem GIDS-Portal eine Web-basierte Übersicht über alle sie betreffenden Alarmmeldungen. Überdies können mit Hilfe des Benutzerportals von Seiten der Ressourcenprovideradministratoren einige Einstellungen vor allem in Hinblick auf Sichtbarkeiten von Alarmmeldungen vorgenommen werden.

2.1.7 AP 7: Kalibrierung des GIDS in Bezug auf das D-Grid Umfeld

2.1.7.1 Beteiligte Projektpartner

- Leibniz-Rechenzentrum (LRZ)
- Regionales Rechenzentrum für Niedersachsen (RRZN)
- DFN-CERT

Leitung: LRZ

Dauer: 12 PM

2.1.7.2 Erzielte Ergebnisse

In diesem Arbeitspaket bestand die Aufgabe darin, die GIDS-Infrastruktur hinsichtlich des produktiven Betriebs im D-Grid vorzubereiten und zu kalibrieren. Hierfür wurden diverse Lasttests sowohl der Infrastruktur als auch der einzelnen Komponenten durchgeführt. Ebenso wurden Export- und Import-Skripte angepasst und erweitert, welche vor und nach der Übertragung über den GIDS-Bus ausgeführt werden. Neben der technischen Zuverlässigkeit der implementierten Lösung wurde ebenso die Umsetzung des Datenschutzkonzepts sichergestellt. Von einem GIDS-spezifischen Sensor werden Angriffversuche aus dem Internet registriert und über die GIDS-Kanäle an alle anderen Sites verteilt. Dabei wurde die datenschutzrechtlich strengste Form erprobt, in der alle Informationen, die potentiell dem Datenschutz widersprechen oder seitens der Ressourcenanbieter sicherheitskritisch sein können, komplett gelöscht werden.

In Zusammenarbeit mit AP 6.4 wurde ein an das D-Grid angepasstes Rollenmodell entworfen und in der Benutzeroberfläche integriert. Das Rollenmodell verwendet in der technischen Umsetzung die Daten der Grid-internen „Grid Resource Registry Service“ (GRRS), in der für Ressourcenanbieter und VO getrennt die entsprechenden Rechte konfiguriert werden können. Weiterhin wurde ein Prototyp eines Klassifikators für IDS-Meldungen entwickelt. Ziel ist eine Abbildung der Meldungen auf Klassen von Angriffen, die in der Bedrohungsanalyse des Projektes festgelegt wurden.

Für die Kalibrierung des GIDS wurden die aktuell erkannten Angriffe ausgewertet. Dabei hat sich bestätigt, dass die IDS (sowohl Snort als auch Prelude-LML) in der Standard-Konfiguration eine hohe Rate von Fehlalarmen produzieren. Auch hat sich gezeigt, dass sich die überwiegende Anzahl der Fehlalarme durch Aggregation und Korrelation vermeiden lässt. Da bestimmte Dienste wie beispielsweise

SSH und FTP in den Grid-Middlewares auf anderen Ports laufen, wurden spezielle Regeln für Snort hinzugefügt. Weiterhin wurden neue Plugins für den Prelude-Correlator implementiert, um insbesondere von den IDS als kritisch eingestufte IDS-Meldungen erkennen zu können. Andere Plugins wurden verbessert, um die Rate der Fehlalarme weiter zu reduzieren. Dies ist insbesondere deshalb wichtig, weil im Portal nur korrelierte Alarme angezeigt werden.

2.1.7.3 Gegenüberstellung mit den vorgegebenen Zielen

Insgesamt hat die Auswertung der IDS-Alarmmeldungen ergeben, dass Angriffe von der eingesetzten Sensoren zuverlässig erkannt werden. Da die IDS-Sensoren auf Linux Systemen liefen, schlugen die Angriffe der Internet Würmer auf Windows Schwachstellen fehl und wurden nicht erkannt. Deshalb wurde die Verbreitung verschiedener Würmer simuliert und deren Erkennung wurde erfolgreich getestet. Auch die Aggregation und Korrelation durch den Prelude-Correlator erzielte die erwarteten Ergebnisse. Zwar konnten False-Positives nicht vollständig vermieden werden, jedoch wurde die Rate im Vergleich zu den rohen Meldungen der IDS deutlich gesenkt. Im Testzeitraum wurde kein lokaler Angriff auf den Grid-Systemen beobachtet. Aus diesem Grund konnte die Erkennung von lokalen Angriffen (z. B. lokale Root Exploits) nicht bewertet werden.

2.1.8 AP 8: Tragfähigkeitsnachweis / Tests der Leistungsfähigkeit

2.1.8.1 Beteiligte Projektpartner

- Leibniz-Rechenzentrum (LRZ)
- Regionales Rechenzentrum für Niedersachsen (RRZN)
- DFN-CERT

Leitung: RRZN

Dauer: 11 PM

2.1.8.2 Erzielte Ergebnisse

Im Rahmen des Arbeitspaketes 8 wurde eine vollständige GIDS-Infrastruktur aufgebaut, die interaktiv auf einem Workshop bei der D-Grid Ergebniskonferenz vorgestellt und unter Mitwirkung der Workshop-Teilnehmer erfolgreich betrieben

wurde. Diese Infrastruktur bestand aus allen nötigen Komponenten wie GIDS-Bus, GIDS-Betreiber, mehreren von den Workshopteilnehmern betreibenen Sensoriken, die stellvertretend für die Ressourcenbetreiber standen, einer kompletten Portallösung und einer simulierten verteilten Netzarchitektur. Weiterhin wurde im Zusammenarbeit mit den Partnern eine Wurm-Simulation eingesetzt, die die Ausbreitung verschiedener Würmer simuliert. Diese Simulation diente einerseits zum Testen und Kalibrieren der Sensorik bezüglich der Ausbreitung eines Internet-Wurms. Auf der anderen Seite wurde die Belastbarkeit der Infrastruktur des GIDS erfolgreich getestet.

Zur Bestätigung der Tragfähigkeit der GIDS-Sensorik wurden die durch Snort und Prelude-LML erkannten Angriffe ausgewertet. Dabei haben sich die für Grid-Systeme sehr kritischen Brute-Force-Angriffe auf schwache SSH-Passwörter als die Kategorie herausgestellt, die mit sehr großen Abstand am häufigsten aufgezeichnet wurde. Dies unterstreicht die Bedeutung dieser Angriffe für die Bedrohung von Grid Systemen. Die beobachteten ICMP-Pings sind zwar in der Mehrzahl keine direkten Angriffe; jedoch wird dies häufig zur Vorbereitung für einen Angriff durchgeführt.

Weiterhin wurden Angriffsmeldungen mittels einer simulierten Ausbreitung des Wurms *Code Red v2* und *Code Red II* beigefügt. Ziel der Simulation war die Reaktion des GIDS in Bezug auf die Robustheit der Nachrichtenübermittlung und die Erkennungsleistung bezüglich der Ausbreitung eines Internet-Wurms zu testen. Die induzierten Daten stellen dabei eine Art zusätzlichen virtuellen Log-Sensor einer Firewall der jeweiligen Domäne dar. Es wurden zusätzlich zu den tatsächlich anfallenden Realdaten alle Access-List-Hits einer zentralen Firewall der jeweiligen Domäne, die durch die Ausbreitung der Wurminstanzen verursacht worden wären, berichtet. Die simulierten Daten der Wurmausbreitung stammen dabei aus der von Harald Schmidt in [24] entwickelten Plattform zur Simulation verschiedener Wurmausbreitungsstrategien.

2.1.8.3 Gegenüberstellung mit den vorgegebenen Zielen

Die Auswertung der Ergebnisse der IDS-Sensorik aller beteiligten GIDS-Partner und der Wurm-Simulation hat gezeigt, dass das GIDS die Anforderungen an die Robustheit der Architektur und Erkennung von Angriffen erfüllt. Dabei hat speziell die Erkennung der simulierten Wurmausbreitung die Vorteile eines föderierten IDS unterstrichen.

2.1.9 AP 9: Produktivführung des GIDS

2.1.9.1 Beteiligte Projektpartner

- Leibniz-Rechenzentrum (LRZ)
- Regionales Rechenzentrum für Niedersachsen (RRZN)
- DFN-CERT

Leitung: LRZ

Dauer: 7,5 PM

2.1.9.2 Erzielte Ergebnisse

Ziel des Arbeitspaketes war die Produktivführung der prototypischen Implementierung des GIDS. Für den Betrieb wurde das weiterentwickelte Portal im DFN-CERT aufgesetzt und an die im DFN-CERT vorherschenden Infrastruktur angepasst:

- Das Portal wurde auf einer eigenen virtuellen Maschine aufgesetzt und die Software für die im DFN-CERT verwendeten OpenSuSE Linux Distributionen paketiert.
- Es wurde eine Infrastruktur aufgesetzt, um optionale Erweiterungen zukünftiger Anpassungen oder Erweiterungen zu testen und in die Softwarepakete zu integrieren, ohne den produktiven Betrieb zu behindern.
- Es wurden weitere Anpassungen an die Infrastruktur des DFN-CERTs vorgenommen. Dadurch kann das GIDS-Portal beispielsweise durch zukünftige Lösungen für die Hochverfügbarkeit profitieren.
- Für den produktiven Betrieb wurden die erweiterten Anforderungen an die Authentifizierung und den Betrieb, wie beispielsweise die Überprüfung von Zertifikats-Sperrlisten, realisiert.
- In Zusammenarbeit mit dem Arbeitspaket 7 wurde das Rechtesystem für den Zugriff auf das Portal erweitert und an die aktuellen Daten des D-Grids angepasst.

Im Portal wurden weitere Suchfunktionen nach IDS-Alarmen hinzugefügt, die die Suche nach IP-Adressen und IDS-Alarmen ermöglichen. Es werden Softwarepakete für Debian Linux zur Verfügung gestellt, die GIDS-Software auf der Seite des Ressourcenproviders bündeln.

Auf der Basis der Kooperation mit dem vom BSI und CERT-Verbund geförderten Frühwarnsystem CarmentiS wurde ein Datenexport zu diesem System realisiert. Dadurch stehen die GIDS-Daten der Frühwarnung zur Verfügung. Ein weiterer Vorteil ist, dass die Daten durch die Kooperation potentiell der Bearbeitung von Sicherheitsvorfällen durch den DFN-Dienst automatische Warnmeldungen zur Verfügung stehen. Aufgrund des zentralen Exportes der Daten steht diese Option jedem Partner des GIDS zur Verfügung.

Die Sensorik der Partner wurde in die produktive Instanz des GIDS integriert, so dass jetzt die Daten der GIDS-Partner einfließen. Datenquellen sind dedizierte Systeme im DFN-CERT, LRZ und RRZN, die Firewalls einschließen, die geblockte Verbindungen protokollieren. Auf der organisatorischen Ebene wurde ein Betriebskonzept für einen GIDS-Dienst erstellt, der Anleitungen für die Bedienung des Portals und für das Aufsetzen und die Anbindung einer administrativen Domäne beinhaltet.

Das GIDS-Portal steht unter `https://www.grid-ids.de/index.php?id=3` bzw. unter `https://gidsportal.dfn-cert.de/` zur Verfügung.

2.1.9.3 Gegenüberstellung mit den vorgegebenen Zielen

Mit dem Abschluss der Arbeitspaketes 9 steht eine produktive Version des GIDS zur Verfügung, die den Ausgangspunkt für einen nachhaltigen Dienst im D-Grid bildet. Im Rahmen des Dienstes kann jeder Teilnehmer am D-Grid mit gültigem D-Grid-Zertifikat auf das Portal zugreifen, durch das die aufgezeichneten Angriffsdaten präsentiert werden. Die Sensorik wird nach Abschluss des Projektes vom LRZ, der LMU in München, dem RRZN und DFN-CERT betrieben, die als Ressourcenprovider am GIDS angeschlossen sind. Damit sind die im Projektplan gestellten Ziele vollständig erfüllt. Um einen nachhaltigen Betrieb anbieten zu können, ist ein zuverlässiger Fortbestand und ein Betriebsmodell des D-Grids notwendig, das speziell die Öffnung des D-Grids für kommerzielle Anwendungen mit einbezieht. Aus diesem Grund wird die weitere Entwicklung des D-Grids abgewartet. Weiterhin ist das Vorhaben und der damit verbundene Betrieb essentiell von zentralen D-Grid-Komponenten wie der GRRS-Datenbank abhängig. Ohne diese ist eine Zuordnung eines Nutzers zu einer bestimmten VO oder auch zu einem Ressourcenprovider nicht mehr möglich. Jedoch haben sind durch die Kooperation mit CarmentiS weitere Möglichkeiten der Verwertung ergeben, die im Projektplan nicht vorgesehen waren. Dies ermöglicht eine zusätzliche Verwendung der GIDS-Daten für die Frühwarnung im Internet und die Bearbeitung von Sicherheitsvorfällen.

2.2 Bewertung der Projektergebnisse

Das hauptsächliche Ziel des GIDS-Projektes war die Etablierung eines föderierten Intrusion Detection Systems für das D-Grid, das als Dienst produktiv betrieben wird. Dieses IDS kann einen wichtigen Beitrag für den sicheren Betrieb des D-Grids beisteuern, insbesondere wenn sich das D-Grid kommerziellen Anwendungen öffnet.

Wie bereits zuvor detailliert beschrieben, umfassten die Arbeiten des Projekts auf der einen Seite einen Architekturentwurf, das Aufsetzen und Anpassen einer Sensorik zum Erkennen aktueller Angriffe, sowie die Erstellung eines Datenschutzkonzepts. Auf der anderen Seite sollte eine Entwicklung der nötigen Komponenten zur Angriffserkennung und zur Darstellung und Information der Nutzer geschaffen werden.

Diese Punkte wurden im Laufe des Projektes vollständig umgesetzt. Neben den konzeptionellen Vorarbeiten, die als Grundlage der späteren Implementierung dienten, wurde zur Darstellung der Angriffsdaten ein zentrales Portal zur Verfügung gestellt, auf das alle Mitglieder im D-Grid zugreifen können. Weiterhin wurde durch den GIDS-Bus und der lokalen GIDS-Komponenten, insbesondere des GIDS-Clients, eine für das D-Grid angepasste Angriffserkennung implementiert, konfiguriert und produktiv in Betrieb genommen. Somit steht mit dem Projektende dem D-Grid das GIDS als produktiver Dienst zur Verfügung. Die im letzten Meilenstein angefügten Dokumente „Anleitung zur Installation der GIDS-Komponenten bei D-Grid-Ressourcenanbietern“ und „Anleitung zur Bedienung des GIDS-Portals“ versetzen die Nutzer in die Lage, diesen neuen angebotenen Dienst ohne großen Einsatz von Personalressourcen nutzen zu können.

Im Rahmen des Projektes wurden die Ergebnisse in den Meilensteinen unter [8–13, 23] veröffentlicht. Weitere Veröffentlichungen der Projektergebnisse fanden auf dem *18. und 19. DFN-Workshop Sicherheit in vernetzten Systemen*, dem *5. DFN-Forum Kommunikationstechnologien*, dem *18th EUNIS Congress*, sowie der *6th International Conference on IT-Security Incident Management and IT Forensics* und in *Cloud, Grid and High Performance Computing: Emerging Applications* statt, so dass aktuelle Entwicklungen sowohl fachlich interessiertem Publikum in Deutschland und Europa präsentiert werden konnte und dass weiterhin eine kritische Diskussion in größerem Rahmen stattfinden konnte. Solche Rückmeldungen sind während der gesamten Projektlaufzeit zeitnah in die weitere Entwicklung mit eingeflossen.

Für Fujitsu Technology Solutions ergeben sich aus GIDS neue Möglichkeiten bei der Planung organisationsübergreifend eingesetzter Intrusion Detection Systeme.

Fujitsu Technology Solutions betreibt derzeit bereits selbst ein verteiltes internes IDS an verschiedenen Standorten und separate Installationen für Kunden, bisher allerdings nicht organisationsübergreifend. Die Projektergebnisse von GIDS legen für Fujitsu Technology Solutions einen verwertbaren Grundstein für interne Diskussionen über den Einsatz und die Möglichkeiten zum Aufbaus eines organisationsübergreifenden Frühwarnsystems, das konform zu firmeninternen Sicherheitsrichtlinien und juristischen Randbedingungen betrieben werden kann. Neben technisch-architekturellen Ansätzen und Möglichkeiten, die durch GIDS aufgezeigt und durch ihre Implementierung und Produktivführung als skalierbar nachgewiesen wurden, sind insbesondere die Arbeiten an den Themengebieten zum Datenschutz und den juristischen Randbedingungen die Grundlage für weitere Arbeiten und Anwendungen für Fujitsu Technology Solutions .

Stonesoft wird die im Projekt ermittelten Anforderungen zur Anpassung und Verbesserung der eigenen Systeme und Produkte nutzen. Das D-Grid fungiert dabei als exemplarisches Einsatzszenario mit seiner Struktur der Koppelung autonomer Organisationseinheiten. Von besonderem Interesse sind für Stonesoft die im Projekt aufgezeigten Möglichkeiten zur Koppelung proprietärer Werkzeuge unter der Nutzung offener und standardisierter Datenformate und Protokolle. Auch die Projektergebnisse in den beiden Bereichen Datenschutz und „Durchsetzung lokaler Sicherheitsrichtlinien bei der organisationsübergreifenden Kooperation von Frühwarnsystemen“ fließen in das Design neuer und verbesserter Stonesoft-Produkte ein. In einem ersten Schritt wird von Stonesoft aktuell untersucht, wie die GIDS-Ergebnisse konkret in das Produkt „Stonesoft IPS“ einfließen können.

Insgesamt wurden alle wissenschaftlichen und technischen Zielsetzungen des Projektes erfolgreich erfüllt.

2.3 Wichtigste Positionen des zahlenmäßigen Nachweises

Der zahlenmäßige Nachweis weist für das Leibniz-Rechenzentrum die Personalmittel für 72 Personenmonate aus, für das Regionales Rechenzentrum für Niedersachsen für 36 Personenmonate und für das DFN-CERT für 36 Personenmonate, die benötigt wurden, um die oben beschriebenen Leistungen zu erbringen, sowie die Reisemittel für die Teilnahme an GIDS Projekttreffen, D-Grid All Hands Meetings und Ergebniskonferenz und den Veranstaltungen und Workshops, bei denen ausgewählte Projektergebnisse präsentiert wurden.

2.4 Notwendigkeit und Angemessenheit der geleisteten Arbeit

Insgesamt folgten die Arbeiten im Projekt den Planungen im Projektantrag und alle Zielsetzungen konnten erfolgreich erreicht werden. Es wurden keine zusätzlichen Ressourcen zum Erreichen der Projektziele benötigt. Die während des Projektes aufgezeichneten Angriffsdaten haben die Relevanz der Arbeiten unterstrichen. Hierbei ist insbesondere die sehr hohe Anzahl an Brute-Force-Angriffen auf schwache Passwörter hervorzuheben, die eine direkte Bedrohung für Grid-Systeme darstellt. Damit stellt die Erkennung und Reaktion auf Angriffe wie im Projektantrag vorgesehen eine wichtige Voraussetzung für den Betrieb von Grids dar. Im Rahmen des Nachweises der Tragfähigkeit wurde gezeigt, dass die Architektur, Sensorik und das GIDS-Portal dafür die Grundlage bieten können.

2.5 Voraussichtlicher Nutzen des Ergebnisses im Sinne der Fortschreibung des Verwertungsplans

Über den im Projektantrag formulierten Verwertungsplan hinaus hat sich eine Kooperation mit der PRESENSE Technologies GmbH mit Bezug zu dem vom BSI und dem deutschen CERT-Verbund initiierten nationalen Frühwarnsystem CarmentiS entwickelt, von der beide Seiten wie nachfolgend beschrieben profitieren können. Wie im Projektantrag vorgesehen ist eine nachhaltige Nutzung des GIDS-Dienstes für die Mitglieder des D-Grids geplant. Diese umfasst die Nutzung der im Projekt entwickelten Software-Komponenten und den Zugriff auf das GIDS-Portal zur Darstellung der IDS-Meldungen. Weiterhin ist vorgesehen, die D-Grid Partner im Falle einer globalen Anomalie, die im Zusammenhang mit einem kritischen, globalen Angriff auf das D-Grid steht, zu warnen. Hier bietet die Zusammenarbeit mit dem nationalen Frühwarnsystem signifikante Vorteile für die Mitglieder des D-Grids, da somit auch neue Angriffstendenzen erkannt werden können, die eventuell erst später ihre Wirkung auf das D-Grid entfalten.

Wirtschaftliche Erfolgsaussichten Um die Erfolgsaussichten einer kommerziellen Verwertung im D-Grid bewerten zu können, muss die zukünftige Situation abgewartet werden. Ist ein Fortbestand des D-Grids gesichert, wird vom DFN-CERT mit der Beteiligung der D-Grid-Betreibergesellschaft ein Geschäftsmodell erarbeitet, um einen kommerziellen Betrieb des GIDS-Dienstes anzubieten. Des

Weiteren ist in diesem Zusammenhang von Bedeutung, ob und in wie weit sich das D-Grid für die kommerzielle Nutzung ihrer Ressourcen öffnet, da gerade kommerzielle Anwender der Sicherheit eine sehr hohe Bedeutung beimessen. Durch die föderative Nutzung des GIDS gibt es bereits heute die notwendigen Schnittstellen, die es gerade kommerziellen Anwendern erlauben würden, Grid-Ressourcen in bestehende Überwachungs- und Sicherheitsmanagementprozesse zu integrieren. Dies stellt somit ein Alleinstellungsmerkmal dar.

Wissenschaftliche und technische Erfolgsaussichten Die Sicherheit von IT-Systemen stellt eine wichtige Grundlage für das Vertrauen bei der sicheren Nutzung von Grid-Ressourcen dar und ermöglicht erst damit die akademische oder kommerzielle Verwertung bzw. Nutzung von Ergebnissen und Diensten. Dabei müssen insbesondere die Verfügbarkeit der Ressourcen sowie die Vertraulichkeit und die Integrität der Daten gewährleistet werden, aber auch die Kontrolle über die Art der Nutzung. Diese wurden in der Vergangenheit durch Angriffe auf Computersysteme im Allgemeinen wie auch auf Grid-Systeme im Speziellen beeinträchtigt. Die Verfügbarkeit wurde beispielsweise durch verteilte Denial of Service (DDoS) Angriffe beeinträchtigt. Weiterhin führten erfolgreiche Angriffe auf Benutzer-Passwörter oder andere Credentials zu unautorisierten Nutzungen und Störungen. Insbesondere erlaubten diese Passwörter Angreifern auch den Zugriff auf vertrauliche Forschungsergebnisse. Aus diesen Gründen kann das GIDS einen wichtigen Beitrag zum notwendigen Vertrauen im D-Grid beitragen, das für die Nutzung der Grid-Ressourcen notwendig ist.

Da die DFN-CERT Services GmbH generell Unterstützung bei der Behandlung sicherheitskritischer Vorgänge bietet, ist eine Nutzung neuer Dienste bzw. die Empfehlung derselben eine Möglichkeit, um Vorfälle bei Nutzern zu verhindern oder zu minimieren, bietet aber darüber hinaus vor allem die Chance, Hilfestellungen noch konkreter und gezielter anzubieten. Bereits durch die während der Projektlaufzeit gewonnenen Erfahrungen und die direkte Kommunikation mit Anwendern und Projektpartnern wird die DFN-CERT Services GmbH noch besser in der Lage sein, auf die neu hinzukommenden speziellen Anforderungen der Grid-Anwender einzugehen. Darüber hinaus bietet sich auf der Basis der entwickelten Softwarekomponenten und dem im D-Grid etablierten Dienst die Chance, generell als eine Trusted Third Party, die rechtlich unabhängig von den Grid-Nutzern und diesen übergeordnet agieren kann, ähnliche Dienste bezogen auf die IT-Sicherheit allgemein anzubieten. Dies bezieht sich beispielsweise auf Erweite-

rungen oder Ergänzungen des DFN-Dienstes der automatischen Warnmeldungen, in dessen Rahmen die GIDS-Daten zukünftig verwertet werden sollen.

Eine weitere Möglichkeit der Verwertung hat sich aus der Kooperation mit der PRESENSE Technologies GmbH bezüglich CarmentiS ergeben. CarmentiS ist ein Frühwarnsystem, das insbesondere ein Lagebild der Bedrohungssituation im Internet erzielt. Durch die Realisierung einer Schnittstelle von GIDS zu CarmentiS lassen sich jetzt auch die Grid-Ressourcen in das Lagebild mit einbeziehen. Auf der anderen Seite erhalten die GIDS-Partner nach Unterzeichnung einer Kooperationsvereinbarung Zugriff auf das CarmentiS Lagebild.

Die in der Projektlaufzeit am LRZ durchgeführten stetigen Verbesserungen und Weiterentwicklungen des Prelude-Frameworks und dessen Komponenten, die als Basis für GIDS dienen, werden unter einer Open-Source-Lizenz veröffentlicht. Um diese Verbesserungen auch einer großen Community zu Gute kommen kann, soll mittelfristig die Integration in das Prelude-Projekt angestrebt werden. Für einen Übergangszeitraum wurde am LRZ ein Git-Server aufgebaut [30], der die Versionierung des Prelude-Projektes unterstützt [29]. Dadurch können Verbesserungen und Patches zeitnah der Community weitergegeben werden, so dass durch diese Änderungen auftretende eventuelle Fehler oder Seiteneffekte frühzeitig erkannt und behoben werden können, bevor sie offiziell in den Entwicklungszweig von Prelude aufgenommen werden. Ebenfalls wurde ein Fork der Software emcast mit initiert, da die Weiterentwicklung dieses Programms seit 2002 nicht mehr vorangetrieben wurde. Durch diese Übergangsmaßnahmen können Fehlerkorrekturen und Verbesserungen sofort eingepflegt werden und interessierten Community-Mitgliedern zugänglich gemacht werden.

Die im Projekt entwickelten Komponenten zur Früherkennung werden im LRZ auch weiterhin produktiv im Einsatz sein und das Sicherheitsniveau im Münchner Wissenschaftsnetz signifikant steigern.

Am LRZ werden die Forschungsergebnisse in Kooperationen mit den Münchner Universitäten in Form von Vorlesungen, Praktika und studentischen Arbeiten eingesetzt und weiterentwickelt. Das Forschungsprojekt dient somit auch dazu, die Lehre anwendungsorientierter ausrichten zu können und somit die Ausbildung der künftigen Informatikergeneration praxisnäher auszurichten.

Schlussendlich wird das LRZ die Forschungsergebnisse des Projektes in zukünftigen Forschungs- und Entwicklungsvorhaben als Basis einsetzen. So ist beispielsweise bei der Präsentation des Projektes auf dem DFN-Forum Kommunikationstechnologien die Frage aufgekommen, das Ergebnis des Projektes auf Cloud-Computing zu übertragen. Weiterhin wurde auf der NGI-DE-Tagung weiterhin die

Idee eingebracht, die im Projekt GIDS entwickelte Infrastruktur auf das von DFN betriebene X-WiN auszudehnen. Dabei würde zu gute kommen, dass das Konzept von GIDS eine strikte Einhaltung der Autonomie der einzelnen Ressourcenanbieter vorsieht. Im X-WiN wäre die Situation ähnlich, da dort die einzelnen Universitäten ebenfalls weiter autonom agieren könnten. Auch eine spätere Ausdehnung auf andere organisationsübergreifende Netzinfrastrukturen und Providerkonstellationen ist denkbar. Zwar würden durch diese Weiterentwicklung die Grid-Aspekte aus der Betrachtung von GIDS fallen, jedoch wären die Anpassungen durchführbar, da die Problemstellungen in einem solchen Szenario vergleichbar sind. Eine andere Fragestellung könnte sein, wie man die in GIDS entwickelte Infrastruktur in europäische Grid-Projekte einbinden kann.

Wissenschaftliche und wirtschaftliche Anschlussfähigkeit Bei der Architektur des GIDS wurden auf der einen Seite die speziellen Anforderungen des Grid-Struktur berücksichtigt, auf der anderen Seite wurde auf bestmögliche Flexibilität geachtet. Deshalb bieten sich für die wissenschaftliche und wirtschaftliche Anschlussfähigkeit mehrere aussichtsreiche Möglichkeiten. Zuerst besteht die Möglichkeit, GIDS neben CarmentiS mit anderen Frühwarnsystemen oder verteilten IDS zu verbinden, um neben Grids auf verschiedenen Gebieten eine verbesserte Erkennung von Angriffen zu erreichen, weil die dazu notwendigen Schnittstellen bereits implementiert sind.

Neben der hauptsächlich vom DFN-CERT vorangetriebenen Kooperation mit dem von der PRESENSE Technologies GmbH betriebenen Projekt CarmentiS können auch schon durch das LRZ initiierte Kooperationen mit dem Fraunhofer-Institut für sichere Informationssysteme und dem Lehrstuhl von Prof. Carle an der Technischen Universität München vertieft werden. Während die Kooperation mit PRESENSE eher den Fokus auf dem Austausch von veredelten und korrelierten Alarmen legt, sind die anderen beiden Kooperationen auf die gemeinsame Nutzung und fortschreitende Weiterentwicklung von Sensoriken angelegt. Insbesondere wurde in Zusammenarbeit mit dem Frauenhofer-Institut ein Honeypotsystem namens Malware Collection Box (MalCoBox) in Betrieb genommen und stetig weiterentwickelt.

Des Weiteren kann GIDS auf andere, verwandte Infrastrukturen übertragen werden. Dabei liegt es nahe, GIDS an Cloud-Architekturen anzupassen. Aufgrund der Virtualisierung der Cloud-Ressourcen ergeben sich neuartige Einsatzgebiete für verteilte IDS. So existiert mit dem Monitor der virtuellen Maschinen neuartige Möglichkeiten zum Einsatz von verteilten IDS. Aufgrund des hohen kommerziellen

Interesses an Cloud-Infrastrukturen ist eine gute kommerzielle Verwertbarkeit der Dienstleistung zu erwarten.

Weiterhin wird das LRZ in der gemeinsamen Angriffserkennung und Frühwarnung des GIDS als Partner bleiben und in diesem Zuge auch die bereitgestellte Hardware für den Betrieb des GIDS weiter betreiben. Diesbezüglich muss jedoch angemerkt werden, dass der Betrieb von GIDS – insbesondere das VO-/mandantenfähige GIDS-Portal – zentrale Komponenten von D-Grid, insbesondere die GRRS-Datenbank, voraussetzt. Ein nachhaltiger Betrieb mit vollem Funktionsumfang kann also nur sichergestellt werden, wenn auch diese anderen D-Grid-Komponenten weiterbetrieben werden, was außerhalb des Verantwortungsbereichs der GIDS-Projektpartner liegt.

2.6 Bekannt gewordener Fortschritt zur Laufzeit des Vorhabens

Zur Laufzeit des Vorhabens wurden keine relevanten Fortschritte auf diesem Gebiet bei anderen Stellen veröffentlicht. Zwar wurde eine Vielzahl an Artikeln veröffentlicht, welche sich dem Themenkomplex annehmen, jedoch bezieht sich der größte Teil eben jener Veröffentlichungen auf Konzepte, die vor Beginn dieses Vorhabens bereits bekannt waren und deutlich divergente Anforderungen an ein Grid-basiertes Intrusion Detection System im Vergleich zu GIDS stellen. Zwei dieser Ansätze sollen im Folgenden vorgestellt und ihre Defizite gegenüber GIDS dargestellt werden.

Ein neuerer Ansatz zur Identifizierung von Angriffen auf mehrere Grid-Ressourcen wird im Artikel [17] vorgestellt. Hierfür wird auf mehrere Intrusion Detection Systeme zurückgegriffen, welche lokal bei den Sites betrieben werden. Diese sollen potenzielle Angriffsdaten an eine zentrale Instanz senden, welche durch Korrelation und mittels statistischer Methoden globale, ressourcenübergreifende Angriffe erkennen kann. Der Nachteile des Ansatzes, eine zentrale Komponente zur globalen Korrelation zu verwenden, wurde jedoch bereits in [23] diskutiert. Bei GIDS wird statt einer zentralen Instanz zur Korrelation und zur Erkennung von Grid-globalen Angriffen ein verteilter Ansatz implementiert. Dies hat den Vorteil, dass bestimmte Sicherheitsvorfälle schon recht früh erkannt werden können, kein potenzieller „Single Point of Failure“ besteht und die Korrelationsalarme durch nur lokal verfügbare Informationen veredelt werden können.

Weiterhin wird in [33] ein weitere Möglichkeit für die Konzeption eines verteilten Grid-basierten Intrusion Detection Systems aufgezeigt. Jede Grid-Site betreibt eigene Intrusion Detection Systeme, welche andere Site bei sicherheitsrelevanten

Vorfällen automatisch identifizieren und alarmieren. Dafür betreibt jede Site einen sogenannten Event Auditor, welcher entsprechende Meldungen sammelt bzw. die Alarmierungen durchführt. Weiterhin besteht eine synchrone, verteilte Datenbank, in der Alarme gesammelt und das Nutzerverhalten teilweise aufgezeichnet wird, um diese Informationen bei der Bewertung neuer Vorfälle zu berücksichtigen. Zur Teilnahme an diesem IDS muss wie bereits erwähnt jede Grid-Site eigene Intrusion Detection Systeme betreiben und ein Abbild der globalen Datenbank speichern. Bei GIDS hingegen muss für die passive Teilnahme ausschließlich ein gültiges Nutzerzertifikat vorhanden sein. Bei einer aktiven Teilnahme an GIDS ist außer selbst eingebrachten IDS- oder Firewall-Daten nur eine Verbindung mit dem GIDS-Bus nötig, was eine relativ niedrige Hürde darstellt, um bereits verwertbare Ergebnisse zu erzielen. Schlussendlich ist auch der Ansatz, die für die Angriffserkennung verwendete Datenbank synchron zwischen allen teilnehmenden Sites zu halten, im praktischen Einsatz nicht umsetzbar. Zum einen würde sich das zu übermittelnde Datenaufkommen deutlich vergrößern, zum anderen haben Datenzulieferer gegebenenfalls ein berechtigtes Interesse, gewisse Alarmmeldungen innerhalb der eigenen Domäne zu belassen. Das würde jedoch im Umkehrschluss bedeuten, dass diese Informationen nicht mehr für die Veredelung von Korrelationsmeldungen verwendet werden könnten.

Zusammenfassend ist somit erkennbar, dass sich die anderen neueren Ansätze entweder auf einem rein akademischen Grad ohne praktische Relevanz bewegen, oder die in GIDS ermittelten Anforderungen nicht erfüllt werden können. Daher sind die Fortschritte nicht relevant für das Projekt gewesen.

2.7 Erfolgte und geplante Veröffentlichung des Ergebnisses

2.7.1 Meilensteinberichte

- Helmut Reiser, Nils gentschen Felde, Felix von Eye, Jan Kohlrausch und Christian Szongott. *Anforderungs- und Kritierienkatalog (MS 6)*. Meilensteinbericht. D-Grid, Jan. 2010. URL: `http://www.grid-ids.de/documents/GIDS_MS6.pdf`

- Wolfgang Hommel, Nils gentschen Felde, Felix von Eye, Jan Kohlrausch und Christian Szongott. *Grobskizze einer Architektur*. Meilensteinbericht. D-Grid, Apr. 2010. URL: `http://www.grid-ids.de/documents/GIDS_MS10.pdf`

- Wolfgang Hommel, Nils gentschen Felde, Felix von Eye, Jan Kohlrausch und Christian Szongott. *Informationsmodell inklusive Datenaustauschformat*. Meilensteinbericht. D-Grid, Juni 2010. URL: `http://www.grid-ids.de/documents/GIDS_MS12.pdf`

- Wolfgang Hommel, Nils gentschen Felde, Felix von Eye, Jan Kohlrausch und Christian Szongott. *Datenschutzmodell für ein Grid-basiertes IDS*. Meilensteinbericht. D-Grid, Juli 2010. URL: `http://www.grid-ids.de/documents/GIDS_MS13.pdf`

- Wolfgang Hommel, Nils gentschen Felde, Felix von Eye, Jan Kohlrausch und Christian Szongott. *Architekturkonzept fur ein Grid-basiertes IDS*. Meilensteinbericht. D-Grid, Okt. 2010. URL: `http://www.grid-ids.de/documents/GIDS_MS16-1.pdf`

- Wolfgang Hommel, Nils gentschen Felde, Felix von Eye, Jan Kohlrausch und Christian Szongott. *Prototypische Implementierung*. Meilensteinbericht. D-Grid, Feb. 2012. URL: `http://www.grid-ids.de/documents/GIDS_MS28.pdf`

- Wolfgang Hommel, Nils gentschen Felde, Felix von Eye, Jan Kohlrausch, Matthias Bräck und Christian Szongott. *GIDS – Produktivsystem*. Meilensteinbericht. D-Grid, Juni 2012. URL: `http://www.grid-ids.de/documents/GIDS_MS36.pdf`

2.7.2 Wissenschaftliche Publikationen

- Nils gentschen Felde, Wolfgang Hommel, Jan Kohlrausch, Jan Köcher, Christian Szongott und Felix von Eye. „Ein föderiertes Intrusion Detection System für das D-Grid“. In: *Sicherheit in vernetzten Systemen: 18. DFN Workshop*. Hrsg. von Christian Paulsen. Norderstedt: Books on Demand, Dez. 2010, I-1–I-21. ISBN: 978-3842343894

- Stefan Metzger, Wolfgang Hommel und Helmut Reiser. „Integriertes Management von Sicherheitsvorfällen“. In: *Sicherheit in vernetzten Systemen: 18. DFN Workshop*. Hrsg. von Christian Paulsen. Norderstedt: Books on Demand, Dez. 2010, D-1–D-21. ISBN: 978-3842343894

- Stefan Metzger, Wolfgang Hommel und Helmut Reiser. „Integrated Security Incident Management – Concepts and Real-World Experiences“. In: *6th*

International Conference on IT-Security Incident Management and IT Forensics. Stuttgart, Mai 2011

- Wolfgang Hommel. „A policy-based security framework for privacy-enhancing data access and usage control in Grids“. In: *Cloud, Grid and High Performance Computing: Emerging Applications*. Hrsg. von Emmanuel Udoh. IGI Global, 2011, S. 118–134. ISBN: 978-1609606039

- Felix von Eye, Stefan Metzger und Wolfgang Hommel. „Innentäter in Hochschulrechenzentren – organisatorische und technische Maßnahmen zur Prävention und Detektion“. In: *Sicherheit in vernetzten Systemen: 19. DFN Workshop*. Hrsg. von Christian Paulsen. Norderstedt: Books on Demand, Jan. 2012, B-1–B-19. ISBN: 978-3844806885

- Nils gentschen Felde, Wolfgang Hommel, Jan Kohlrausch, Helmut Reiser, Christian Szongott und Felix von Eye. „Das Datenschutzkonzept für das föderierte Frühwarnsystem im D-Grid und seine technische Umsetzung“. In: *5. DFN-Forum Kommunikationstechnologien – Beiträge der Fachtagung*. Hrsg. von Paul Müller, Bernhard Neumair, Helmut Reiser und Gabi Dreo Rodosek. GI-Edition – Lecture Notes in Informatics (LNI); 203. Bonn: Gesellschaft für Informatik, Mai 2012, S. 53–62. ISBN: 978-3885792970

- Wolfgang Hommel, Silvia Knittl und Felix von Eye. „XaaS Cloud Service Strategy for Dynamic Higher Education Institution IT Infrastructures“. In: *Book of abstracts – a 360° perspective on IT/IS in higher education*. Hrsg. von Benjamim Fonseca. EUNIS 2012 – 18th EUNIS Congress. Vila Real: Universidade de Trás-os-Montes e Alto Douro, Juni 2012, S. 177–178. ISBN: 978-9897040863

- Wolfgang Hommel, Stefan Metzger, Helmut Reiser und Felix von Eye. „Log file management compliance and insider threat detection at higher education institutions“. In: *Book of abstracts – a 360° perspective on IT/IS in higher education*. Hrsg. von Benjamim Fonseca. EUNIS 2012 – 18th EUNIS Congress. Full paper: `http://www.eunis.pt`. Vila Real: Universidade de Trás-os-Montes e Alto Douro, Juni 2012, S. 115–116. ISBN: 978-9897040863

- Nils gentschen Felde, Wolfgang Hommel, Jan Kohlrausch, Helmut Reiser, Christian Szongott und Felix von Eye. „A Grid-based Intrusion Detection System (GIDS)“. In: *Book of abstracts – a 360° perspective on IT/IS in higher education*. Hrsg. von Benjamim Fonseca. EUNIS 2012 – 18th EUNIS

Congress. Vila Real: Universidade de Trás-os-Montes e Alto Douro, Juni 2012, S. 185–186. ISBN: 978-9897040863

2.7.3 Projektinterne Veranstaltungen

Während der Projektlaufzeiten wurden die folgenden projektinternen Veranstaltungen durchgeführt:

- *24. Juli 2009, Garching*
  Kick-Off Meeting
- *13. Januar 2010, Garching*
  Projekttreffen
- *30. Juni 2010, Hamburg*
  Projekttreffen
- *30. September 2010, Göttingen*
  Projekttreffen im Anschluss an den 5. D-Grid Security Workshop
- *16. Februar 2011, Hamburg*
  Projekttreffen im Anschluss an den 18. DFN Workshop
- *20. Mai 2011, Garching*
  Projekttreffen im Anschluss an die NGI-DE-Jahrestagung 2011
- *12. – 13. Juli 2011, Hannover*
  Projekttreffen
- *10. – 11. Oktober 2011, Garching*
  Projekttreffen
- *05. – 06. März 2012, Hamburg*
  Vorbereitungstreffen zur D-Grid Ergebniskonferenz
- *21. März 2012, Bonn*
  Projekttreffen im Anschluss an die D-Grid Ergebniskonferenz
- *25. – 27. Juni 2012, Garching*
  Projektabschlusstreffen

2.7.4 Eigene Vorträge auf Konferenzen/Workshops

- *4. D-Grid Security Workshop 2009*, Göttingen
  15. – 16. Oktober 2009
  Helmut Reiser: *GIDS Projektvorstellung* (`https://www.grid-ids.de/documents/Reiser-GIDS_Projektvorstellung_01.pdf`)

- *Open Grid Forum (OGF) 28*, München
  15. – 18. März 2010
  Nils gentschen Felde: *The GIDS project* (`http://www.ogf.org/OGF28/materials/1993/OGF_GIDS.ppt`)

- *9th RoEduNet International Conference*, Sibiu, Rumänien
  24. – 26. Juni 2010
  Wolfgang Hommel: *Securing Research and Education Networks: Challenges and Solutions* (`http://roedu2010.ulbsibiu.ro/news/lecture_3_abstract.pdf`)

- *5. D-Grid Security Workshop 2010*, Göttingen
  29. – 30. September 2010

  1. Felix von Eye: *Architekturvorschlag und Implementierungsüberblick* (`https://www.grid-ids.de/documents/vonEye-GIDS_ArchUeberblick.pdf`)
  2. Jan Kohlrausch: *Das Datenschutzkonzept für GIDS* (`https://www.grid-ids.de/documents/Kohlrausch-GIDS_DatenSchKonzept.pdf`)

- *18. DFN Workshop „Sicherheit in vernetzten Systemen“*, Hamburg
  15. – 16. Februar 2011
  Stefan Metzger: *Integriertes Management von Sicherheitsvorfällen* (`http://www.dfn-cert.de/dokumente/workshop/2011/folienmetzger.pdf`)

- *6th International Conference on IT Security Incident Management & IT Forensics*, Stuttgart
  10. – 12. Mai 2011
  Stefan Metzger: *Integrated Security Incident Management – Concepts and real-world Experiences* (`http://www1.gi-ev.de/fachbereiche/sicherheit/fg/sidar/imf/imf2011/slides/1-02_IMF2011_Metzger.pdf`)

- *NGI-DE-Jahrestagung 2011*, Garching
  18. – 20. Mai 2011

Felix von Eye: *Grid Intrusion Detection im D-Grid* (`https://www.grid-ids.de/documents/vonEye-GIDS_allgemein.pdf`)

- *19. DFN Workshop „Sicherheit in vernetzten Systemen“*, Hamburg
  21. – 22. Februar 2012
  Felix von Eye: *Innentäter in Hochschulrechenzentren – organisatorische und technische Maßnahmen zur Prävention und Detektion* (`http://www.dfn-cert.de/dokumente/workshop/2012/Folien_vonEye.pdf`)

- *D-Grid Ergebniskonferenz*, Bonn
  19. – 21. März 2012

  1. Matthias Bräck, Nils gentschen Felde, Jan Kohlrausch, Christian Szongott, Felix von Eye: *gemeinsamer Workshop der Projekte GIDS und GapSLC*
     - Implementierungs- und Integrationsüberblick (`https://www.grid-ids.de/documents/ergebniskonferenz/GIDS_allgemein.pdf`)
     - Umsetzung des Datenschutzkonzeptes (`https://www.grid-ids.de/documents/ergebniskonferenz/GIDS_Datenschutzkonzept.pdf`)
     - Realisierung einer Benutzeroberfläche (`https://www.grid-ids.de/documents/ergebniskonferenz/GIDS_Portal.pdf`)
     - „Hands-On Tutorial“ & Life-Demo
  2. Poster: *Ein Gridbasiertes, föderiertes Intrusion Detection System zur Sicherung der D-Grid Infrastruktur* (`https://www.grid-ids.de/documents/ergebniskonferenz/GIDS-Poster-DINA1.pdf`)

- *5. DFN-Forum 2012*, Regensburg
  21. – 22. Mai 2012
  Jan Kohlrausch: *Das Datenschutzkonzept des Grid-IDS Projektes und dessen Umsetzung* (`http://www.uni-regensburg.de/veranstaltungen/dfn2012/medien/vortraege/08_gids-datenschutzkonzept.pdf`)

- *EUNIS'12 - A 360° perspective on IT/IS in Higher Education*, Vila Real, Portugal
  20. – 22. Juni 2012

  1. Felix von Eye: *Log file management compliance and insider threat detection at higher education institutions* (`http://www.eunis.pt/images/docs/presentations/P3D-2.pptx`)

2. Poster: *A Grid-based Intrusion Detection System (GIDS)* (`http://www.eunis.pt/`)

Weiterhin wurde am 30.05.2012 eine Anwenderschulung für interessierte GIDS-Nutzer aus dem Großraum München gehalten. Den Inhalt dieser Schulung oder die oben genannten Vorträge können jederzeit wieder vor einem interessierten Publikum wiederholt werden oder gegebenenfalls an neue Randbedingungen angepasst werden.

Abbildungsverzeichnis

Literatur

[1] Ong Tian Choon und Azman Samsudin. „Grid-based Intrusion Detection System“. In: *Proceedings of the 9th Asia-Pacific Conference on Communications (APCC)*. Bd. 3. Sep. 2003, S. 1028–1032.

[2] N. gentschen Felde. „Einsatz der graphbasierten Meldungsstrukturanalyse in domänenübergreifenden Meta-IDS“. In: *Lecture Notes in Informatics — Informatik 2005, Informatik LIVE!* Band 2 P–68. Bonn, Germany: Gesellschaft für Informatik, Sep. 2005, S. 653–657.

[3] N. gentschen Felde, M. Jahnke, P. Martini und J. Tölle. „Impact of Sanitized Message Flows in a Cooperative Intrusion Warning System“. In: *Proceedings of the 25th Military Communications Conference (MILCOM 2006)*. Bd. 2006. Washington, DC, USA, Okt. 2006, S. 1–7.

[4] Nils gentschen Felde, Wolfgang Hommel, Jan Kohlrausch, Jan Köcher, Christian Szongott und Felix von Eye. „Ein föderiertes Intrusion Detection System für das D-Grid“. In: *Sicherheit in vernetzten Systemen: 18. DFN Workshop*. Hrsg. von Christian Paulsen. Norderstedt: Books on Demand, Dez. 2010, I-1–I-21. ISBN: 978-3842343894.

[5] Nils gentschen Felde, Wolfgang Hommel, Jan Kohlrausch, Helmut Reiser, Christian Szongott und Felix von Eye. „A Grid-based Intrusion Detection System (GIDS)“. In: *Book of abstracts – a 360° perspective on IT/IS in higher education*. Hrsg. von Benjamim Fonseca. EUNIS 2012 – 18th EUNIS Congress. Vila Real: Universidade de Trás-os-Montes e Alto Douro, Juni 2012, S. 185–186. ISBN: 978-9897040863.

[6] Nils gentschen Felde, Wolfgang Hommel, Jan Kohlrausch, Helmut Reiser, Christian Szongott und Felix von Eye. „Das Datenschutzkonzept für das föderierte Frühwarnsystem im D-Grid und seine technische Umsetzung“. In: *5. DFN-Forum Kommunikationstechnologien – Beiträge der Fachtagung*. Hrsg. von Paul Müller, Bernhard Neumair, Helmut Reiser und Gabi Dreo Rodosek. GI-Edition – Lecture Notes in Informatics (LNI); 203. Bonn: Gesellschaft für Informatik, Mai 2012, S. 53–62. ISBN: 978-3885792970.

[7] Wolfgang Hommel. „A policy-based security framework for privacy-enhancing data access and usage control in Grids“. In: *Cloud, Grid and High Performance Computing: Emerging Applications*. Hrsg. von Emmanuel Udoh. IGI Global, 2011, S. 118–134. ISBN: 978-1609606039.

[8] Wolfgang Hommel, Nils gentschen Felde, Felix von Eye, Jan Kohlrausch, Matthias Bräck und Christian Szongott. *GIDS – Produktivsystem*. Meilensteinbericht. D-Grid, Juni 2012. URL: http://www.grid-ids.de/documents/GIDS_MS36.pdf.

[9] Wolfgang Hommel, Nils gentschen Felde, Felix von Eye, Jan Kohlrausch und Christian Szongott. *Architekturkonzept fur ein Grid-basiertes IDS*. Meilensteinbericht. D-Grid, Okt. 2010. URL: http://www.grid-ids.de/documents/GIDS_MS16-1.pdf.

[10] Wolfgang Hommel, Nils gentschen Felde, Felix von Eye, Jan Kohlrausch und Christian Szongott. *Datenschutzmodell für ein Grid-basiertes IDS*. Meilensteinbericht. D-Grid, Juli 2010. URL: http://www.grid-ids.de/documents/GIDS_MS13.pdf.

[11] Wolfgang Hommel, Nils gentschen Felde, Felix von Eye, Jan Kohlrausch und Christian Szongott. *Grobskizze einer Architektur*. Meilensteinbericht. D-Grid, Apr. 2010. URL: http://www.grid-ids.de/documents/GIDS_MS10.pdf.

[12] Wolfgang Hommel, Nils gentschen Felde, Felix von Eye, Jan Kohlrausch und Christian Szongott. *Informationsmodell inklusive Datenaustauschformat*. Meilensteinbericht. D-Grid, Juni 2010. URL: http://www.grid-ids.de/documents/GIDS_MS12.pdf.

[13] Wolfgang Hommel, Nils gentschen Felde, Felix von Eye, Jan Kohlrausch und Christian Szongott. *Prototypische Implementierung*. Meilensteinbericht. D-Grid, Feb. 2012. URL: http://www.grid-ids.de/documents/GIDS_MS28.pdf.

[14] Wolfgang Hommel, Silvia Knittl und Felix von Eye. „XaaS Cloud Service Strategy for Dynamic Higher Education Institution IT Infrastructures“. In: *Book of abstracts – a 360° perspective on IT/IS in higher education*. Hrsg. von Benjamim Fonseca. EUNIS 2012 – 18th EUNIS Congress. Vila Real: Universidade de Trás-os-Montes e Alto Douro, Juni 2012, S. 177–178. ISBN: 978-9897040863.

[15] Wolfgang Hommel, Stefan Metzger, Helmut Reiser und Felix von Eye. „Log file management compliance and insider threat detection at higher education institutions“. In: *Book of abstracts – a 360° perspective on IT/IS in higher education*. Hrsg. von Benjamim Fonseca. EUNIS 2012 – 18th EUNIS Congress. Full paper: http://www.eunis.pt. Vila Real: Universidade de Trás-os-Montes e Alto Douro, Juni 2012, S. 115–116. ISBN: 978-9897040863.

[16] K. Hwang, Y. Kwok, S. Song, M. Cai, R. Zhou, Y. Chen, Y. Chen und 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*. Mai 2005.

[17] Catalin Leordeanuand, Levni Arif und Valentin Cristea. „Correlation of Intrusion Detection Information in Grid Environments“. In: *Proceedings of the fourth International Conference on Complex, Intelligent and Software Intensive Systems (CISIS 2010)*. Bd. 2010. Krakow, Poland, Feb. 2010, S. 463–468.

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

[19] Fang-Yie Leu, Jia-Chun Lin, Ming-Chang Li und Chao-Tung Yang. „A Performance-Based Grid Intrusion Detection System“. In: *Proceedings of the 29th International Computer Software and Applications Conference (COMPSAC)*. Bd. 1. Juli 2005, S. 525–530. ISBN: 0-7695-2413-3.

[20] Stefan Metzger, Wolfgang Hommel und Helmut Reiser. „Integriertes Management von Sicherheitsvorfällen“. In: *Sicherheit in vernetzten Systemen: 18. DFN Workshop*. Hrsg. von Christian Paulsen. Norderstedt: Books on Demand, Dez. 2010, D-1–D-21. ISBN: 978-3842343894.

[21] Stefan Metzger, Wolfgang Hommel und Helmut Reiser. „Integrated Security Incident Management – Concepts and Real-World Experiences“. In: *6th International Conference on IT-Security Incident Management and IT Forensics*. Stuttgart, Mai 2011.

[22] Jiancheng Ni, Zhishu Li, Jirong Sun und 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)*. Juni 2007, S. 97–106.

[23] Helmut Reiser, Nils gentschen Felde, Felix von Eye, Jan Kohlrausch und Christian Szongott. *Anforderungs- und Kritierienkatalog (MS 6)*. Meilensteinbericht. D-Grid, Jan. 2010. URL: `http://www.grid-ids.de/documents/GIDS_MS6.pdf`.

[24] Harald Schmidt. „Simulation und Erkennung der Ausbreitungsstruktur von Würmern“. Magisterarb. Universität Bonn, Sep. 2002.

[25] Alexandre Schulter, Julio Albuquerque Reis, Fernando Koch und 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)*. Apr. 2006.

[26] Alexandre Schulter, Fabio Navarro, Fernando Koch und Carlos Becker Westphall. „Towards Grid-based Intrusion Detection“. In: *Proceedings of the 10th Network Operations and Management Symposium (NOMS)*. Apr. 2006, S. 1–4. ISBN: 1-4244-0142-9.

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

[28] Mohamed F. Tolba, Mohammad S. Abdel-Wahab, Ismail A. Taha und 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*. Cardiff, UK, Mai 2005.

[29] Felix von Eye und Wolfgang Hommel. *Das Security Information and Event Management System (SIEM) Prelude*. URL: `http://git.lrz.de/prelude/`.

[30] Felix von Eye, Wolfgang Hommel und Martin Roll. *Git-Server des Leibniz-Rechenzentrums*. URL: `https://git.lrz.de`.

[31] Felix von Eye, Stefan Metzger und Wolfgang Hommel. „Innentäter in Hochschulrechenzentren – organisatorische und technische Maßnahmen zur Prävention und Detektion“. In: *Sicherheit in vernetzten Systemen: 19. DFN Workshop*. Hrsg. von Christian Paulsen. Norderstedt: Books on Demand, Jan. 2012, B-1–B-19. ISBN: 978-3844806885.

[32] Jun Wang und Luigi Lo Iacono. „Intrusion Detection and Tolerance in Grid-based Applications“. In: *Proceedings of the First International Workshop on Security, Trust and Privacy in Grid Systems (Grid-STP 2007)*. Nice, France, Mai 2007.

[33] Carlos B. Westphall, Carla M. Westphall, Fernando L. Koch, Carlos O. Rolim, Kleber M. Vieira, Alexandre Schulter, Shirlei A. Chaves, Jorge Werner, Rafael S. Mendes, Rafael B. Brinhosa, Guilherme A. Geronimo und Rafael R. Freitas. „Management and Security for Grid, Cloud and Cognitive Networks“. In: Bd. 8. 2011, S. 8–21. URL: `http://www.fsma.edu.br/si/edicao8/FSMA_SI_2011_2_Principal_6.pdf`.