Integriertes Management von Sicherheitsvorfällen

S. Metzger, W. Hommel, H. Reiser
Leibniz-Rechenzentrum (LRZ)
Boltzmannstraße 1, 85748 Garching b. München
[metzger|hommel|reiser]@lrz.de

Zusammenfassung

In diesem Artikel wird ein integrierter, praxiserprobter Ansatz für das Management von Sicherheitsvorfällen vorgestellt. Das Computer Security Incident Response Team (CSIRT) wird dabei in die Lage versetzt, IT-Security-Events über verschiedene Meldewege hinweg zu korrelieren und die Vorfälle einheitlich zu klassifizieren.

Abhängig von der Klassifikation des Vorfalls besteht die Möglichkeit der manuellen Intervention oder aber der vollautomatischen Reaktion, beginnend bei einfacher Benachrichtigung der zuständigen Systemverantwortlichen bis hin zur Sperrung von kompromittierten Systemen und ganzen Subnetzen. Als Basis für die Vorfallsbearbeitung dient ein formal spezifizierter Security Incident Response (SIR) Prozess, der klare Verantwortlichkeiten und die notwendige Abfolge von Bearbeitungsschritten definiert; er stellt damit eine best- und schnellstmögliche Reaktion auf eine besonders ressourcenschonende Art und Weise sicher.

1 Motivation

Durch den Gewinn, der aus dem Verkauf von personenbezogenen Daten und dem Vermieten von Botnetzen erzielt werden kann, sind mit dem Internet verbundene IT-Systeme für Angreifer ein immer lohnenderes Ziel. Denkt man an dieser Stelle aber nur an weltweit operierende Unternehmen einerseits und virenverseuchte Privatanwender-PCs andererseits, so irrt man: Auch öffentliche Einrichtungen wie Behörden und Hochschulen rücken immer stärker in den Fokus von Angreifern – zum Teil mit spektakulären Erfolgen [Chi10]. Ziel solcher Angriffe sind zum Beispiel die personenbezogenen Daten von Mitarbeitern bzw. Studenten wie E-Mail-Adressen und Matrikelnummer-Listen. Neben dem Schaden, der durch den reinen Datenverlust und die Kompromittierung von Systemen entsteht, ist meist der Imageschaden der für die IT-Sicherheit verantwortlichen Einrichtung, insbesondere für das zuständige Hochschulrechenzentrum, immens.

Zugriffe von außen, d.h. über das Internet, werden meist bereits durch verschiedene Werkzeuge wie Firewalls und IDS/IPS-Systeme geschützt. Angreifer können aber auch im Inneren

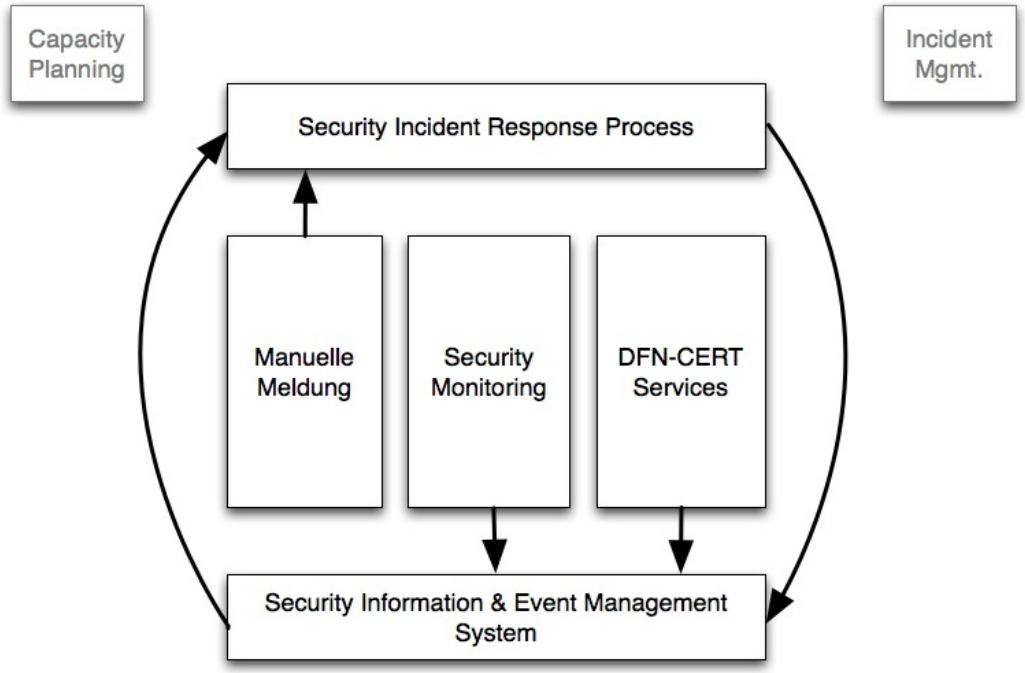

Abbildung 1: Integriertes Management von Sicherheitsvorfï¿½llen (allgemein)

aktiv werden. Hier sind neben unzufriedenen Mitarbeitern z.B. auch experimentierfreudige Studenten, Gäste oder Konferenzteilnehmer, die über WLAN temporären Zugriff auf das Netz erhalten, in Angreifermodellen zu berücksichtigen. Während die Serversysteme und Arbeitsplatzrechner der Mitarbeiter in der Regel zentral verwaltet und somit auch regelmäßig gepatcht werden, ist eine zentral angestoßene, zeitnahe Aktualisierung von studentischen Geräten (PCs, Notebooks, Netbooks, Smartphones, . . .) oder von Gästen meist gar nicht oder nur sehr eingeschränkt möglich.

Aus diesem Grund greifen ausschließlich präventive Maßnahmen offensichtlich zu kurz und nur für einen Teil der an ein Netz angeschlossenen IT-Systeme. Notwendig sind deshalb zusätzlich strukturiert ablaufende detektierende und reaktive Maßnahmen, die sich aus den in Abbildung 1 dargestellten Bausteinen zusammensetzen.

Die übergeordnete Koordination erfolgt durch einen definierten Security Incident Prozess (basierend auf dem Paradigma der prozessorientierten Intervention), der neben Verantwortlichkeiten auch das Vorgehen bei der Bearbeitung von sicherheitsrelevanten Ereignissen festlegt und die gesamte Vorfallsbearbeitung steuert. Dabei sind insbesondere folgende zueinander komplementäre Wege für die Meldung von Security-Events zu berücksichtigen:

- Manuelle Meldung per E-Mail, Telefon oder Fax durch Administratoren, andere Computer Security Incident Response Teams (CSIRTs) oder Strafverfolgungsbehörden; dies ist insbesondere im Umfeld von Grid-Projekten (organisationsübergreifende Verbünde von Rechen- und Speicherressourcen) eine essenzielle Meldequelle.

- Meldedienste des DFN-CERT, insbesondere der Dienst *Automatische Warnmeldungen*.

- Verschiedene Security-Monitoring-Mechanismen zur Detektion von Schadsoftware und ungewöhnlichem, überwiegend unerlaubtem Kommunikationsverhalten.
- Eine zentrale Auswertung sicherheitsrelevanter Ereignisse durch ein Security Information und Event Management System mit den Möglichkeiten zur Korrelation sowie zur automatischen Reaktion.

Unsere Zielsetzung ist es, diese verschiedenen Meldewege so miteinander zu kombinieren, dass eine schnellstmögliche Reaktion im Rahmen eines ganzheitlichen, integrierten Managements von Sicherheitsvorfällen erreicht wird. Besonderes Augenmerk liegt hierbei auf einer zeitnahen, bestenfalls in Echtzeit ablaufenden automatischen Reaktion bei minder schweren Vorfällen, wodurch sich der notwendige Personaleinsatz minimieren lässt.

Dieser Artikel beschreibt unseren bereits erfolgreich praktisch eingesetzten Lösungsweg und ist wie folgt gegliedert: Im nächsten Abschnitt werden die von uns genutzten externen Informationsquellen – insbesondere der Meldedienst des DFN-CERT – skizziert. In Abschnitt 3 stellen wir das Münchner Wissenschaftsnetzes (MWN) und die sich dort ergebenden Herausforderungen beim Sicherheitsmanagement vor. Desweiteren erfolgt an dieser Stelle eine Erläuterung der aktuell am Leibniz-Rechenzentrum (LRZ) eingesetzten Werkzeuge für das Security-Monitoring des MWN. In Abschnitt 4 wird der am LRZ erfolgreich eingeführte, formale Security Incident Response Prozess vorgestellt. Anschließend beschreiben wir die Kombination dieser Mechanismen und Meldewege im Hinblick auf das integrierte Management von Sicherheitsvorfällen und die Einbettung in das ganzheitlich zu betrachtende Information Security Management am LRZ. Zum Abschluss geben wir nach einer kurzen Zusammenfassung einen Ausblick auf die von uns geplanten zukünftigen Entwicklungen.

2 DFN-CERT Services: Sicherheitsmeldungen

Das bereits sehr umfangreiche Dienstleistungsangebot des DFN-CERT besteht zum einen aus proaktiven Diensten (Informationen zu Schwachstellen) und zum anderen aus reaktiven Diensten (Automatische Warnmeldungen, im Folgenden als AW-Dienst bezeichnet) [DC10]. Der Schwerpunkt der proaktiven Dienste liegt auf der Beseitigung von Schwachstellen in Betriebssystemen und einzelnen Applikationen, bevor diese aktiv von Angreifern ausgenutzt werden. Neu im Angebot der präventiven Dienste ist der so genannte Netzwerkprüfer; er besteht aus einem NMAP-basierten Scan-Werkzeug, mithilfe dessen Einrichtungen ihre Netzbereiche von außen scannen können. Damit lässt sich mit sehr einfachen Mitteln feststellen, welche Systeme und welche darauf angebotenen Dienste prinzipiell erreichbar sind und ob die grundlegenden Sicherheitsregeln (z.B. kein SSH-Zugang zu Webservern über das Internet) eingehalten werden. Dieser Dienst ergänzt somit lokal durchgeführte Scans, die aufgrund unterschiedlicher Firewall-Regeln jedoch typischerweise auch zu partiell anderen Ergebnisse führen, und ist somit ein unverzichtbares Hilfsmittel für regelmäßige Vulnerability Assessments.

Zumindest für viele der zentral verwalteten, am Netz angeschlossenen Systeme ist die Beseitigung von Schwachstellen durch ein regelmäßiges, automatisiertes Einspielen von Security-Patches, die auf zentral aufgestellten Update-Servern zur Verfügung gestellt werden, sehr einfach möglich. Durch den Einsatz solcher relativ einfacher proaktiver Maßnahmen lassen sich

die Eintrittswahrscheinlichkeiten für einige Klassen von Sicherheitsvorfällen und damit die Schäden für einzelne Systeme bzw. Dienste und damit für die gesamte Einrichtung bereits deutlich reduzieren.

Wenn es trotz dieses Angebots an Hilfsmitteln zur Prävention und der allgemein gebotenen Vorsicht dennoch zu einer Vireninfektion bzw. allgemein zu einer Kompromittierung eines IT-Systems gekommen ist, leistet der DFN-CERT AW-Dienst eine sehr wichtige Hilfestellung. Grundlage für diesen reaktiven Service bilden die kontinuierliche Auswertung verschiedenster Quellen und insbesondere der Betrieb eigener Sensoren, sog. Honeypots, beim DFN-CERT. Honeypots täuschen potentiellen Angreifern bewusst Dienste vor, in denen Schwachstellen vorhanden sind. Damit lässt sich Schadsoftware und vor allem deren Verhalten im Detail analysieren. Einrichtungen des DFN erhalten somit neben der Meldung einer auffälligen IP-Adresse aus einem ihrer Netzbereiche zusätzlich detaillierte Informationen zu der auf dem infizierten System installierten Schadsoftware, z.B. deren Namen. Damit lassen sich gezielt Gegenmaßnahmen, wie der Einsatz spezieller Removal-Tools, einleiten.

Die Auffälligkeiten werden durch den AW-Dienst klassifiziert, so dass ähnliche Fälle bzw. Verhaltensmuster derselben Klasse zuordenbar sind und damit denselben Meldungstyp zugewiesen bekommen. Derzeit unterscheidet der DFN-CERT rund zehn Meldungstypen, z.B. Angriff, Bot, Portscan oder Spam-Beschwerde. Bei bestimmten Meldungstypen, z.B. Bot, erfolgt desweiteren eine Einteilung in Malwaretypen, welche dann z.B. den Namen der Schadsoftware, z.B. Conficker oder Mebroot, enthält. Hier ein kurzer Auszug aus einer durch den AW-Dienst verschickten E-Mail:

```
System:       xxx.xxx.xxx.xxx
Meldungstyp:  Bot
Zeitstempel:  2010-07-17 09:31:12 GMT+0200 (Sommerzeit)
Beschreibung: Auf dem System scheint eine Bot-Software betrieben zu
              werden, die versucht, einen HTTP-basierten Bot-Netz
              Control-Server zu erreichen. Zu den unterschiedlichen
              Malwaretypen finden Sie unter der folgender Webseite mehr
              Informationen: http://www.cert.dfn.de/index.php?id=bot

TCP Quellport   TCP Zielport   Malwaretyp    HTTP Request
-------------------------------------------------------------------------
1667            80            Conficker     GET /search?q=0 HTTP/1.0
3812            80            Conficker     GET /search?q=0 HTTP/1.0
```

Neben den automatischen Meldediensten und dem präventiven Netzwerkprüfer-Service meldet der DFN-CERT schwerwiegende Sicherheitsvorfälle und -ereignisse direkt an vorher benannte Vertreter der Einrichtung per E-Mail oder Telefon. Komplementär dazu besteht auch die Möglichkeit, intern in einer Einrichtung detektierte Vorfälle an den DFN-CERT zu melden. Damit ist es möglich, ein nationales Lagebild zu zeichnen bzw. das tatsächliche, möglicherweise organisationsübergreifende Ausmaß eines Angriffs festzustellen. Der DFN-CERT unterstützt die Einrichtung anschließend bei der Bearbeitung und Lösung eines solchen Vorfalls. Neben der Kompetenz und Erfahrung der DFN-CERT-Mitarbeiter erweist es sich dabei häufig als äußerst vorteilhaft, dass der DFN-CERT einen sehr guten Überblick über aktuelle, ähnliche Vorfälle bei den anderen angebundenen Einrichtungen hat.

3 Proaktives Netz- und Systemmonitoring im MWN durch das LRZ

Das Münchner Wissenschaftsnetz verbindet überwiegend Standorte der Münchner Hochschulen (Technische Universität München (TUM), Ludwig-Maximilians Universität (LMU), Hochschule München (HM), FH Weihenstephan-Triesdorf). Außerdem sind noch einige außeruniversitäre Einrichtungen daran angeschlossen. Diese sind größtenteils über die gesamte Region Münchens verteilt, umfassen aber auch weitere Standorte in ganz Bayern. Die Gesamtzahl ans MWN angeschlossener Endgeräte wird derzeit mit rund 79.500 (Stand: April 2010) angegeben, wobei diese Anzahl durch nur temporär angeschlossene Systeme von Studenten, Gästen und z.B. Konferenzteilnehmer tatsächlich deutlich höher liegt. Die Anzahl steigt zudem stetig an [LR10a].

Durch seine Struktur kann das MWN nicht wie ein übliches Unternehmensnetz betrieben werden. Die administrative Verantwortung des LRZ für das MWN endet nämlich an der Netzdose. Welche Systeme dort angebunden werden, entscheiden die Institute und Lehrstühle selbst und tragen auch die administrative Verantwortung für die Endsysteme. Trotz dieser verteilten Netzstruktur und der sehr großen Anzahl an angeschlossenen Endgeräten, die überwiegend dezentral administriert werden, versucht das LRZ seit längerer Zeit, sowohl die eigenen als auch die für andere Einrichtungen betreuten Systeme vor Angriffen zu schützen.

Daneben versucht es, Angriffe bzw. bereits Angriffsversuche, die von LRZ-betreuten oder an das MWN angeschlossenen Systemen ausgehen, weitestgehend zu verhindern. Zumindest sollten deren Auswirkungen und der in diesem Zusammenhang möglicherweise entstandene Schaden minimiert werden.

In diesem Abschnitt werden die derzeit eingesetzten Mechanismen im Detail vorgestellt:

- Netzbasiertes Intrusion Detection System (IDS) am Internet-Übergang (X-WiN)
- NAT-Gateway NAT-o-MAT
- E-Mail-Monitoring mittels Accounting
- Auswertung von NetFlow-Daten durch NfSen

Die Detektion von sicherheitsrelevanten Ereignissen alleine reicht jedoch nicht aus; vielmehr sind eine automatische Weiterverarbeitung, Information der zuständigen Administratoren und eine zeitnahe automatische Reaktion notwendig. Dies wird durch Einsatz eines Security Information und Event Management Systems erreicht.

3.1 SNORT - Intrusion Detection am X-WiN

Das bekannte und weltweit sehr häufig eingesetzte Open-Source Network Intrusion Detection System SNORT [Sou10] wird am LRZ z.B. zur Überwachung des ein- und ausgehenden Verkehrs am X-WiN-Übergang eingesetzt und dort zur Erkennung von bekannten Angriffen und

kompromittierten bzw. wurm-infizierten Systemen genutzt. Der Verkehr wird per SPAN-Port an die SNORT-Maschinen weitergeleitet und dort analysiert. Die Analyse besteht bei SNORT im Wesentlichen aus dem Vergleich der Pakete und deren Inhalte mit definierten Pattern.

Der Verbreitungsgrad von SNORT trägt auch dazu bei, dass die Software und die Regelsätze ständig weiterentwickelt werden, um auch auf neuartige Angriffsmethoden geeignet reagieren zu können. Dass eine Software von einer breiten Nutzergemeinde eingesetzt und auch gepflegt und stetig erweitert wird, ist ein sehr wichtiges Entscheidungskritierium am LRZ. Dabei werden allgemein verfügbare Regelsätze der SNORT-Community mit selbstentwickelten Regeln kombiniert eingesetzt, um auch bei Auftreten speziell für das LRZ wichtiger Ereignisse einen Alarm zu generieren. Um einige Beispiele für selbsterstellte Regeln zu nennen, werden externe wie auch interne SSH-Attacker, die Systeme innerhalb des LRZ oder MWN bzw. externe Systeme auf Port 22 zu erreichen versuchen („scannen“) genauso detektiert wie interne Systeme, auf denen auf einem TCP-Port ungleich 21 ein FTP-Server läuft. Auch wenn von extern ausgeführte SSH-Scans alltäglich sind, werden diese meist mit Dictionary-Attacks kombiniert, um schwache Passworte von häufig verwendeten (Standard-)Kennungen, wie *root*, *admin*, *guest* etc. zu brechen, und stellen demnach eine potentielle Gefahr dar. Interne SSH-Attacker, die (Scan-)Angriffe aus dem MWN heraus starten, sind mit hoher Wahrscheinlichkeit mit einer Schadsoftware infiziert und können mithilfe dieses Monitoring-Mechanismus auf sehr einfache Weise detektiert werden.

Erheblich erschwert wird die signaturbasierte Erkennung mit SNORT durch die hohe Bandbreite von 10 Gbit/s am X-WiN-Übergang. Daher werden auf der derzeit eingesetzten Mehrprozessormaschine mehrere Instanzen (aktuell: 8) von SNORT parallel gestartet, da die Software selbst noch nicht multithread-fähig ist. Desweiteren wurden verschiedene Tuning-Einstellungen am Treiber der verwendeten Netzwerkkarten vorgenommen.

Um den zu analysierenden Verkehr pro Instanz zu reduzieren, erfolgt eine Aufteilung auf Basis von Berkeley Packet Filters (BPF) [MJ93]. Die jeweiligen Filter wurden empirisch ermittelt und werden regelmäßig überprüft. Der Verkehr wird nach unterschiedlichen Protokollen (z.B. TCP, UDP, ICMP oder IPv6), bestimmten IP-Adressbereichen und einzelnen Ports (z.B. HTTP, SSH) in etwa gleich große Teile aufgesplittet. Hier eine Filterregel für HTTP-Traffic:

```
ip and ( <subnetze>) and tcp and ( port 80 or port 8080 or port 8180 )
```

Aufgrund dieser einfachen filterbasierten Aufteilung des Traffics ist jedoch der Einsatz der erwähnten SNORT-Community Rules out-of-the-box nicht mehr möglich, denn diese fassen Regeln nach Angriffstypen und nicht nach verwendeten Protokollen oder Ports zusammen. Entsprechend mussten Mechanismen entwickelt werden, die die Community-Rules parsen, zerlegen und geeignet wieder zusammenfügen, damit jede gestartete SNORT-Instanz für sich ein minimales Ruleset verwendet. Dies hat insbesondere positive Auswirkungen auf die Performanz jeder gestarteten Instanz und damit auch auf die Analysezeit. Da diese Vorgehensweise jedoch einen sehr hohen, meist manuellen, administrativen Aufwand erfordert, überlegt das LRZ derzeit, ob die filterbasierte Lösung zur Aufteilung des Traffics nicht weiter optimiert werden könnte, zum Beispiel durch ein Aufsplitten des Verkehrs bereits am Router.

3.2 NAT-o-MAT - NAT-Gateway und Security-Monitoring

Eine weitere sehr einfache Möglichkeit, interne IT-Systeme vor Angriffen aus dem Internet zu schützen, ist der Einsatz von privaten IP-Adressen. Eine direkte Kommunikation mit Systemen im Internet und damit ein Angriff ist dadurch nicht möglich. Nachteil ist, dass auch die Nutzung von z.B. im Internet angebotenen Diensten auf diese Weise ebenfalls nicht möglich ist. Früher verwendete Proxy-Server mußten von den Nutzern meist mühevoll konfiguriert werden, was zum einen umständlich und zum anderen sehr fehleranfällig war. Um diesem Umstand Rechnung zu tragen, wurde am LRZ ein NAT-Gateway entwickelt, das einerseits private in öffentliche IP-Adressen umsetzt und gleichzeitig Aufgaben eines Security-Gateways wahrnimmt, um automatisch Bandbreitenregelung durchzuführen und diverse Angriffsarten (Portscans, (D)DoS und Spam-Angriffen) zu verhindern (siehe [LR10b, FBSR06]).

Basis für das Security-Monitoring bildet ein ratenbasierter Mechanismus. Bei Überschreitung von definierten Grenzwerten, z.B. 100 Pakete pro Sekunde, erhält das Quellsystem einen sog. „Strafpunkt“. In Abhängigkeit der Strafpunktanzahl je definiertem, gleitendem Zeitfenster wird der Internetzugang temporär gesperrt, bis die Strafpunktanzahl unter den Grenzwert sinkt. Der Nutzer wird per E-Mail und per Webseite automatisch über die Sperrung informiert.

```
Gesperrt seit / Blocked since 15.11.10 05:20
Überschreitungen   Protokoll Zielport und Grund der Sperrung
Number of hits     Protocol  Destination port and suspension reason
111                UDP       4600-4699 - Edonkey Filesharing
30                 UDP       7560
30                 UDP       5514
30                 UDP       54067
30                 UDP       4600-4699 - Edonkey Filesharing
30                 UDP       43793
30                 UDP       37283
```

An einer Weiterentwicklung des NAT-o-MAT wird aktuell intensiv gearbeitet. So wurde das Lastverteilungssystem, das bisher von policy-based Routing (PBR) auf den Core-Routern abhängig war, erneuert. Desweiteren wurde die nicht mehr weiterentwickelte Klassifizierung von Peer-to-Peer-Protokollen entfernt und soll mittelfristig durch eine SNORT-basierte Lösung ersetzt werden. Damit bietet das NAT-Security-Gateway zusätzlich auch Intrusion Detection Funktionen, was positive Auswirkungen zum einen auf die Flexibilität der Detektionsmöglichkeiten hätte und zum anderen das IDS am X-WiN-Übergang entlasten würde.

3.3 E-Mail-Monitoring mittels Accounting

Das E-Mail-Security-Monitoring versucht durch Auswertung von Accounting-Daten, Spamversendende Systeme im Münchner Wissenschaftsnetz zu identifizieren. Häufigste Ursache dafür, dass ein System plötzlich beginnt, eine sehr große Anzahl von E-Mails und möglicherweise Spam zu senden, ist die Infektion mit bestimmten Arten von Schad- bzw. insbesondere Botsoftware.

Mithilfe eines ratenbasierten Monitoringmechanismus wird jede Mailverbindung in einem bestimmten Zeitfenster gezählt. Bei Überschreiten individuell konfigurierbarer Schwellwer-

te wird ein Alarm generiert. Betrachtet werden derzeit zwei unterschiedliche Zeitintervalle, fünf Minuten und eine Stunde. Für Standard-Systeme sind je zwei Schwellwerte definiert. Bei Soft-Events, d.h. 20 Mails in 5 Minuten oder 80 Mails pro Stunde wird eine Warnung an die Verantwortlichen verschickt. Bei Hard-Events, d.h. 300 Mails in 5 Minuten oder 1000 Mails pro Stunde wird das entsprechende System automatisch gesperrt. Für jedes Intervall kann der Systembetreuer den Grenzwert aber auch individuell festlegen.

```
Monitoring-Details
==================

Rechner:                [xxx.xxx.xxx.xxx]

Monitoring-Intervall:   5 Minuten  vor  20.07.2010  10:30:28
Mail-Verbindungen:      1616
```

Ein größeres, temporär auftretendes E-Mail-Aufkommen, z.B. der Versand eines monatlichen Newsletters, kann damit mit geringem Aufwand von einer irrtümlichen Alarmierung ausgeschlossen werden.

Dedizierte E-Mail-Server, die über das gesamte MWN verteilt von den einzelnen Instituten selbst betrieben werden und bei denen ein sehr hohes Mail-Aufkommen normal ist, wurden in eine Ausnahmeliste aufgenommen. Die Pflege dieser Liste und damit der zugehörigen Schwellwerte obliegt den zuständigen Netz- und Systemadministratoren.

Die Erkennung von Spam-sendenden Systemen mittels des bereits erwähnten Intrusion Detection Systems SNORT wurde in Erwägung gezogen und prototypisch implementiert. Eine derartige Vorgehensweise hat sich jedoch in der Praxis nicht bewährt. Die Anzahl irrtümlich als Spam-Sender erkannter Systeme war deutlich höher als bei dem erfolgreich eingesetzten ratenbasierten Mechanismus. Auch der Pflegeaufwand (Ausnahmeliste, individuelle Grenzwerte) musste bei der SNORT-basierten Lösung größtenteils durch Personal des LRZ erfolgen, so dass das Verfahren insgesamt nicht attraktiv war.

3.4 NfSen - Analyse von NetFlow-Daten

Immer stärker in den Fokus am LRZ wandert die Analyse von NetFlow-Daten zum Zweck des Security-Monitorings und damit der Erkennung von Angriffen. Das IDS erkennt signaturbasiert nur bekannte Angriffe, wohingegen mithilfe geeigneter Auswertemechanismen NetFlow-Daten nutzbar sind, um Verkehrsanomalien und Zero-Day-Attacken zu erkennen. Besonders im Vordergrund stehen aktuell die Erkennung von Botnetzkommunikation und die Identifikation von Spam-sendenden Systemen über IPv6 und Teredo [Hui06].

NfSen bietet eine webbasierte Schnittstelle für die NetFlow-Toolsammlung *nfdump* und erlaubt damit auf komfortable Weise die Analyse von NetFlow-Daten. Die Einsatzmöglichkeiten von NfSen und NFDUMP wurden 2005 von Peter Haag auf dem 16th TF-CSIRT Meeting [Haa05] im Detail vorgestellt. Durch die Konfiguration von unterschiedlichen Profilen, sortiert nach Flows, Paketen und übertragenem Volumen und Aufteilung nach verschiedenen Protokollen lassen sich verschiedene Sachverhalte übersichtlich darstellen. Die Analyse der Daten

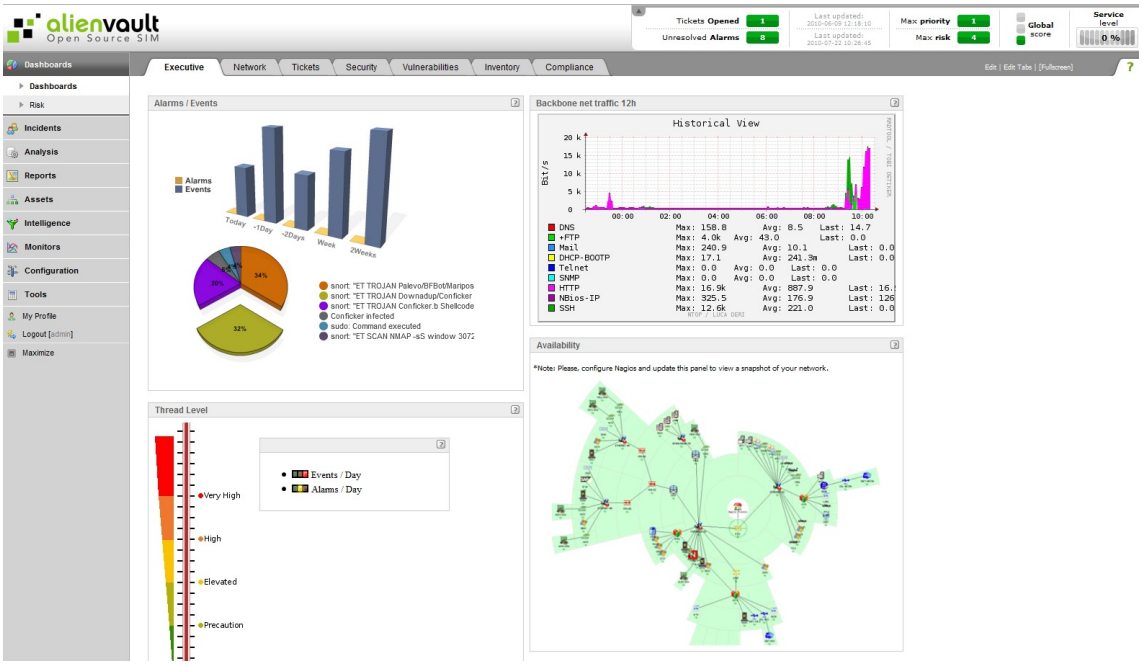

Abbildung 2: Integrierte, frei konfigurierbare Dashboards in OSSIM

erfolgt mittels einer speziellen Filter-Syntax. Somit ist durch Verwendung von Schlüsselwörtern wie *ip*, *net* oder *dst port* die Konfiguration von Filtern sehr einfach möglich. Filter werden einerseits für eine manuell angestoßene Auswertung und andererseits innerhalb eines integrierten Alerting-Mechanismus eingesetzt.

3.5 OSSIM - Security Information & Event Management

Das Open Source Security Information Management (OSSIM) System der Firma Alienvault [Ali10] wurde bereits im Rahmen eines Vortrags von Matthias Hofherr und Peter Wimmer auf dem DFN-CERT Workshop 2009 [Hof09] erwähnt. OSSIM erlaubt die zentrale Sammlung, Korrelation und Auswertung von sicherheitsrelevanten Ereignissen. Die Auswertung erfolgt dabei zum einen manuell durch effiziente Suchfunktionen. So lassen sich die Ereignisse nach Sensoren, Ereignis-ID, Source-IP-Adresse, usw. filtern und sortieren und als Datei exportieren. Über das integrierte Asset-Management lassen sich einzelne Hosts, Subnetze oder ganze Netze zu Host- bzw. Netzgruppen zusammenfassen, was die Übersichtlichkeit stark erhöht. Frei konfigurierbare Dashboards, wie in Abbildung 2 zu sehen sind, und automatisierte Erstellung und Versand von Reports, z.B. Top-10 Attacker, die einen groben Überblick über das aktuelle Sicherheitsniveau geben, runden die Lösung ab.

Durch die Eventkorrelation ist es besonders einfach möglich, sicherheitsrelevante Ereignisse zu priorisieren. Besonders interessant ist dabei die letztgenannte Variante, die Korrelation von Events verschiedener Quellen. Damit ist es möglich, die durch das IDS gemeldeten Ereignisse mit Schwachstellen auf dem angegriffenen Zielsystem zu korrelieren. IDS-Events können trotz hoher IDS-Severity irrelevant sein, falls auf dem System der angegriffene Service, das betroffene Betriebssystem oder eine nicht verwundbare, da bereits aktualisierte Software-Version installiert ist.

Eine weitere, nennenswerte Stärke von OSSIM liegt in der Möglichkeit, nahezu in Echtzeit automatisiert zu reagieren. Das Spektrum möglicher Reaktionen beginnt bei einer einfachen E-Mail-Benachrichtigung eines Administrators und erreicht durch die automatisierte Ausführung von Skripten höchste Flexibilität.

OSSIM stellt am LRZ die zentrale Auswerteinstanz für alle sicherheitsrelevanten Ereignisse, die von internen Monitoring-Mechanismen detektiert werden, dar. Es wurden eine Reihe von Korrelationsdirektiven neben den bereits integrierten erstellt, um auf spezielle Ereignisse adäquat reagieren zu können. Mittels definierter Policies wird, falls bestimmte (korrelierte) Ereignisse auftreten, automatisiert reagiert. Dabei wird das komplette Spektrum möglicher Reaktionen, abhängig von der Event-Severity, ausgenutzt.

4 Der LRZ Security Incident Response Prozess

Neben den Monitoringsystemen und den vom DFN-CERT übermittelten Informationen steht noch eine wichtige dritte Datenquelle für Hinweise auf Sicherheitsvorfälle zur Verfügung: Die manuellen Meldungen durch lokale Systemadministratoren und Dienstverantwortliche, die beispielsweise bei der Kontrolle von Protokolldateien oder beim Arbeiten mit dem jeweiligen System auf sicherheitsrelevante Besonderheiten aufmerksam geworden sind. In diesem Abschnitt skizzieren wir den Mitte 2010 am LRZ formal eingeführten Prozess zur Bearbeitung von Security Incidents. Bei der Definition des Prozesses wurde bereits auf Konformität mit dem Standard ISO/IEC 27001 [ISO05c] geachtet.

Zur Einbettung in die IT-Managementlandschaft am LRZ ist anzumerken, dass daran gearbeitet wird, die Zuverlässigkeit und Verfügbarkeit der erbrachten IT-Dienste auf Basis eines prozessorientierten IT Service Managements (ITSM) noch weiter zu verbessern. Nach einer grundlegenden Orientierung an den Best Practices, die von ITILv3 [oGCO07] vorgegeben werden und allgemein bekannt sind, ist die Zertifizierung nach dem ITSM-Standard ISO/IEC 20000 [ISO05a, ISO05b] eines der zentralen aktuellen Themen bei der strategischen Weiterentwicklung des LRZ. Eine wesentliche Voraussetzung hierfür ist, dass Prozesse und Arbeitsabläufe nicht nur dokumentiert sind und reproduzierbar ablaufen, sondern auch einer kontinuierlichen Verbesserung unterzogen werden. Der ITSM-Teilbereich Incident Management befasst sich unter anderem mit der Annahme von kunden- und anwenderseitigen Meldungen über Dienststörungen und deren schnellstmöglicher Beseitigung. Neben Benutzeranfragen, die vom First Level Support direkt beantwortet oder fachlich an den Second Level Support eskaliert werden, sind zwei speziellere Arten von Incidents zu berücksichtigen: Major Incidents, z.B. beim Komplettausfall eines zentralen Dienstes mit einer Vielzahl betroffener Anwender, und Security Incidents, zu deren Bearbeitung neben den Infrastruktur- und Dienstbetreibern auch Sicherheitsexperten hinzugezogen werden müssen. Dabei ist prinzipiell zu beachten, dass ein Security Incident einen Major Incident nach sich ziehen kann, z.B. wenn ein kompromittiertes System vom Netz genommen werden muss; in der Regel treten jedoch reine Security Incidents wesentlich häufiger auf als Major Incidents.

Für die Meldung sicherheitsrelevanter Vorfälle durch LRZ-Mitarbeiter wurden zunächst eine Sammelrufnummer und eine E-Mail-Adresse definiert, damit Vorfallsmelder insbesondere in dringenden Fällen direkt mit einem LRZ-CSIRT-Mitglied, also einem Ansprechpartner

mit einschlägiger Sicherheitskompetenz, in Kontakt gebracht werden. Obwohl der klassische First Level Support in diesem Fall bewusst umgangen wird, wird z.B. durch die aktuell noch in Implementierung befindliche Integration der Vorfallsbearbeitung ins hausweit eingesetzte Trouble Ticket System sichergestellt, dass alle Incidents unabhängig von Typ und Meldeweg einheitlich dokumentiert werden.

Mit der Meldung eines potenziellen Sicherheitsvorfalls wird der Security Incident Response (SIR) Prozess instanziiert, der im Wesentlichen wie in Abbildung 3 dargestellt aus den Phasen Klassifikation, Eskalation, Analyse, Diagnose, Lösung und Abschluss besteht. Diese nachfolgend noch näher beschriebenen Abläufe sind dabei in folgenden Formen dokumentiert:

- LRZ-Administratoren und -Dienstverantwortliche haben ein bewusst knapp gehaltenes Merkblatt zur Verfügung, das die Kontaktinformationen und die wichtigsten zu meldenden Daten sowie Empfehlungen zu Erstreaktionen und Verhaltensmaßnahmen im Ernstfall enthält.

- Die Prozessbeschreibung, die dem LRZ-CSIRT vorliegt, ist mit über 20 Seiten relativ ausführlich. Sie enthält neben der Spezifikation der Zuständigkeiten und Abläufe auch Verweise auf weitere Dokumente und Verfahrensbeschreibungen, z.B. Best Practices zur grundlegenden IT-forensischen Analyse kompromittierter Systeme.

- Um in der Hitze des Gefechts den Überblick nicht zu verlieren, verwendet das LRZ-CSIRT eine rund fünfseitige Checkliste, in der die wesentlichen Prozessschritte nochmals kompakt zusammengefasst sind.

Bei der Erstanalyse werden die gemeldeten Daten, die beispielsweise die Kontaktinformationen des Vorfallsmelders und eine Beschreibung des identifizierten Sicherheitsvorfalls enthalten sollen, auf Vollständigkeit geprüft und es wird eine initiale Klassifikation vorgenommen. Hierzu wird unter anderem geklärt, wie viele Systeme betroffen sind, ob es sich dabei z.B. um LRZ-interne Server oder Grid-Systeme handelt, welche Dienste betroffen sind und welche Dienstabhängigkeiten bestehen, wo der vermeintliche Standort des Angreifers ist und um welche Art von Angriff es sich handelt; ebenso wird geklärt, ob Zusammenhänge mit bereits bekannten Sicherheitsvorfällen bestehen könnten. Auf dieser Basis erfolgt die Einteilung in eine der vier Prioritätsklassen *niedrig, mittel, hoch* und *sehr hoch*. In der höchsten Stufe wird der Vorfall zum Major Incident ausgeweitet. Als *Standard Security Incident* (SSI) werden im Laufe der Zeit auch ausgewählte Varianten von wiederholt auftretenden sicherheitsrelevanten Vorfällen spezifiziert, für die der Analyse-, Diagnose- und Lösungsweg immer gleich sind, so dass bestimmte Vereinfachungen im Prozessablauf vorgenommen werden können. Beispielsweise werden Brute-Force-Angriffe zum Erraten von SSH-Zugangspasswörtern als SSI behandelt, wenn die Angriffe nicht von einem Rechner im MWN ausgehen und auch nicht gezielt Kennungen nach dem LRZ-Namensschema angreifen. Dadurch kann die relative Vielzahl an Angriffen, deren Erfolgsaussichten und damit Risiko als vernachlässigbar erachtet werden, effizient gehandhabt werden. Gleichzeitig bleibt aber sichergestellt, dass die Vorfälle erfasst und wie unten beschrieben bei der Planung weiterer Sicherheitsmaßnahmen berücksichtigt werden können. Sofern sich im Verlauf der Bearbeitung des Sicherheitsvorfalls neue Erkenntnisse ergeben, kann sich die Klassifikation auch ändern.

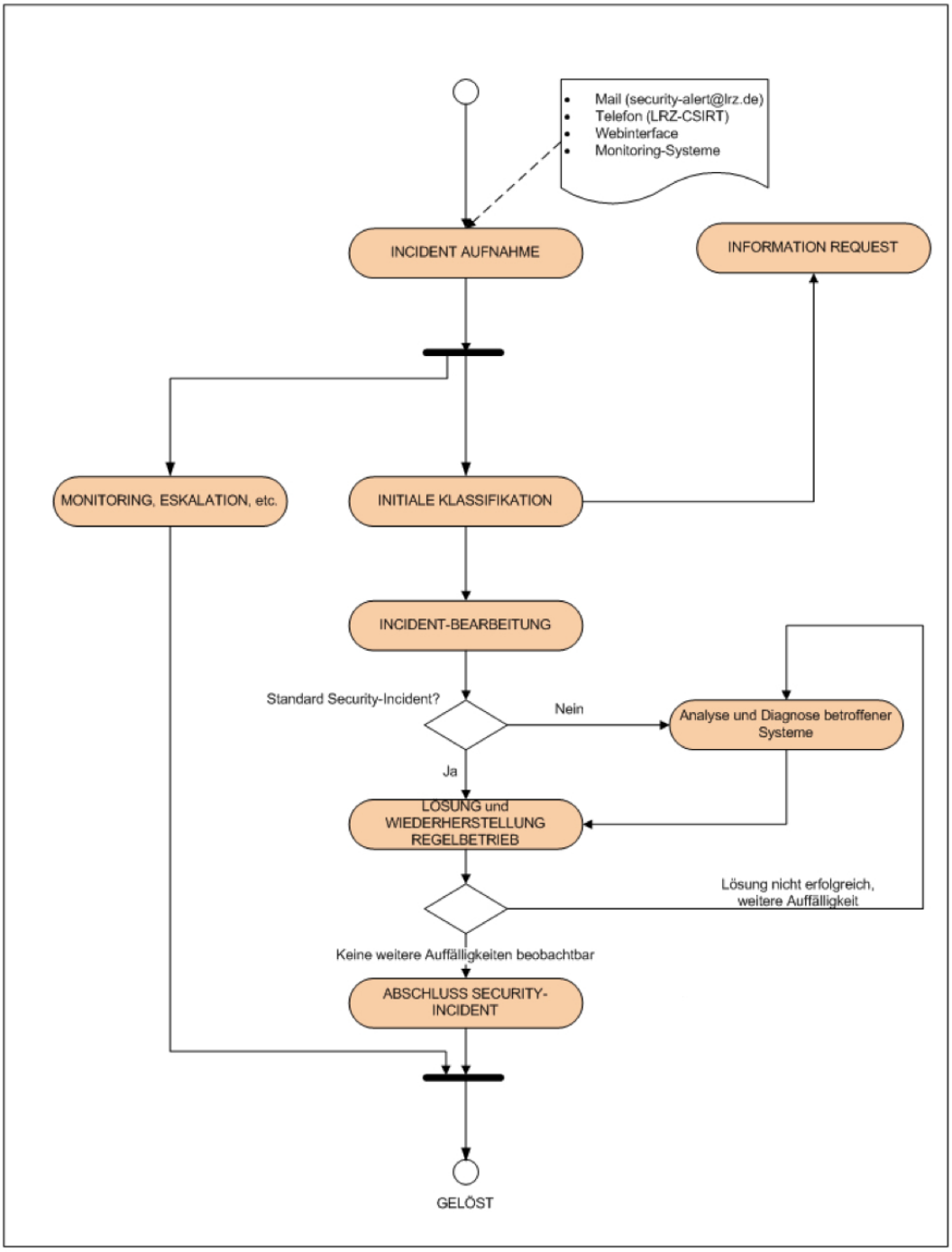

Abbildung 3: Prinzipieller Ablauf des LRZ Security Incident Response Prozesses

Für den Fall, dass es sich um einen individuell zu analysierenden Sicherheitsvorfall handelt, kommt ein vom Bewertungsschema für andere, d.h. nicht sicherheitsspezifische Incidents abweichendes Verfahren zur Feststellung von Auswirkung und Priorität (engl. *impact* und *urgency*) zum Einsatz. Die Einstufung der Auswirkung eines Vorfalls ergibt sich dabei aus einer Gewichtungsformel für die erläuterten Klassifizierungskriterien. Allerdings werden Sicherheitsvorfälle generell als dringend eingestuft. Durch Festlegung der Incident-Priorität wird nicht nur die interne Abarbeitungsreihenfolge beeinflusst, sondern z.B. auch über die im Rahmen von Service Level Agreements (SLAs) zugesicherten Reaktionszeiten entschieden und festgelegt, ob der Vorfall so gravierend ist, dass die LRZ-Leitung schnellstmöglich über den Vorfall informiert werden muss.

Das weitere Vorgehen wird dann von einem pro Vorfall zu bestimmenden Security Incident Coordinator (SIC) koordiniert, der für die Dauer der Bearbeitung des Sicherheitsvorfalls mit ausgewählten Entscheidungsbefugnissen ausgestattet ist und zusammen mit dem CSIRT und gegebenenfalls weiteren Personen wie dem Vorfallsmelder bzw. den Dienstadministratoren die einzuleitenden Maßnahmen festlegt. Diese umfassen beispielsweise das Trennen der Netzverbindung der betroffenen Systeme, die Beweissicherung durch Backups oder – bei virtuellen Maschinen – Snapshots, erste forensische Analysen inklusive der Auswertung von Sicherheits-, Netz- und System-Monitoringdaten, die fachliche oder hierarchische Eskalation sowie die lückenlose Dokumentation der Bearbeitungsvorgänge. Zwei wesentliche Ziele sind dabei insbesondere auch der kontinuierliche Informationsaustausch mit dem Vorfallsmelder und die Sicherstellung, dass eine möglichst baldige Rückkehr zum Regelbetrieb ermöglicht wird. Auch nach der erfolgreichen Aufklärung von Vorfällen werden die entsprechenden Systeme noch einige Tage unter intensivere Beobachtung gestellt, um zu erkennen, ob sich der Vorfall eventuell trotz der getroffenen Maßnahmen wiederholt oder ob noch weitere Auswirkungen an den Tag treten.

Nach größeren Zwischenfällen sowie in regelmäßigen Abständen werden Reviews durchgeführt, um einerseits zu diskutieren, ob und wie der Prozess als Ganzes sowie die in ihm beschriebenen Teilabläufe weiter verbessert werden können. Andererseits wird in Form einer Trendanalyse ermittelt, welche Konsequenzen aus den bisherigen Sicherheitsvorfällen zu ziehen sind, um die präventiven Sicherheitsmechanismen und die proaktiven Maßnahmen z.B. zum Monitoring der Systeme zu verbessern, um kontinuierlich zur Verbesserung des Gesamtsicherheitsniveaus beitragen zu können.

5 Zusammenführung der Meldewege und integriertes Management von Sicherheitsvorfällen

Wie in den vorherigen Abschnitten beschrieben wurde, existieren somit am LRZ drei unterschiedliche Wege, über die sicherheitsrelevante Ereignisse oder Sicherheitsvorfälle gemeldet werden:

- Automatisch generierte und versandte Warnmeldungen des DFN-CERT
- Durch verschiedene interne Monitoring-Mechanismen detektierte und von einer zentralen SIEM-Lösung (OSSIM) korrelierte Ereignisse

- Manuelle Meldung per E-Mail oder Telefon an das LRZ-CSIRT

Diese gilt es nun geeignet zusammenzuführen, um eine best- und damit schnellstmögliche Reaktion zu erreichen. Unsere Zielsetzung ist es, alle Meldungen an einer zentralen Stelle, einem derzeit noch in der Einführungsphase befindlichen ISO/IEC 20000 konformen Trouble Ticket System zusammenzuführen. Als minder schwer eingestufte Ereignisse sind dabei vollautomatisch zu verarbeiten; es sind also insbesondere auch gezielte, automatische Gegenmaßnahmen einzuleiten. Das erzeugte Ticket dient dem CSIRT im Idealfall dann nur zum Tracking des Bearbeitungsstatus, beispielsweise wenn auf Rückmeldungen durch einen Systemverantwortlichen gewartet wird.

In diesem Abschnitt wird unser Ansatz für das integrierte Management von Sicherheitsvorfällen im Detail beschrieben. Dabei wird zunächst auf die automatisierte Verarbeitung der Warnmeldungen des DFN-CERT eingegangen. Abschnitt 5.2 erläutert die zentrale Auswertung der durch die internen Monitoring-Mechanismen detektierten Ereignisse und die eingesetzten automatischen Reaktionsmöglichkeiten, sowie einige kleinere Probleme, die es am LRZ im Speziellen zu lösen galt. Im Anschluss an die automatisch ablaufenden Reaktionsmöglichkeiten wird in Abschnitt 5.3 die manuelle, aber strukturiert ablaufende Bearbeitung von Vorfällen und die dabei zum Einsatz kommenden Werkzeuge beschrieben. Abschliessend wird in Abschnitt 5.4 das Zusammenspiel der verschiedenen Meldewege und Überwachungsmechanismen an einem Beispiel veranschaulicht.

5.1 Auswertung der Automatischen Warnmeldungen des DFN-CERT

Dank der DFN-CERT-Dienste bekommt das LRZ-CSIRT bei auffälligem Kommunikationsverhalten von IT-Systemen innerhalb des MWN eine Benachrichtigung über eine potenzielle Kompromittierung eines Systems per E-Mail zugesandt. Diese Meldungen werden auf Basis des zusätzlich enthaltenen, XML-basierten Formats skriptgesteuert ausgewertet und weiterverarbeitet. Dadurch ist eine Weiterleitung der Information an die jeweils zuständigen Netz- und Systemadministratoren, insbesondere bei Systemen innerhalb des MWN auf sehr einfache und ressourcenschonende Weise möglich. Die Weiterleitung erfolgt auf Basis der MWN-Netzdokumentation, in der bestimmte Parameter wie z.B. die E-Mail-Adressen der Administratoren oder der grobe Standort des Systems eingetragen sind (vgl. [LR10a]).

Die Verantwortlichen ausgewählter Subnetz-Bereiche (z.B. Kliniken mit eigenen Betriebsgruppen) erhalten die Automatischen Warnmeldungen, die ihren Zuständigkeitsbereich betreffen, direkt. Das LRZ-CSIRT wird parallel dazu per E-Mail informiert und kann dadurch den Fortschritt der Bearbeitung des Vorfalls überwachen.

Leider bietet der Service derzeit noch keine Echtzeit-Alarmierung und damit die Möglichkeit zu einer sehr zeitnahen Reaktion. Insbesondere nur temporär angeschlossene Systeme, z.B. private Rechner von Studenten, Gästen oder Konferenzteilnehmern, die meist über WLAN verbunden sind, werden zwar detektiert, das Einleiten von gezielten Gegenmaßnahmen ist jedoch nur eingeschränkt möglich, da der Zeitversatz momentan zu groß ist.

Die Auswertung der Warnmeldungen am LRZ dient deshalb einerseits zur Überprüfung interner Mechanismen und deren Erkennungsqualität und andererseits als gute und sehr einfache Möglichkeit, eigene Mechanismen an bestimmten Stellen gezielt geeignet zu erweitern.

5.2 Detektion durch interne Monitoring-Mechanismen und automatische Reaktion durch SIEM

Wie in Abschnitt 3 beschrieben werden am LRZ verschiedene Monitoring-Werkzeuge zur Detektion von sicherheitsrelevanten Ereignissen eingesetzt. Nach der Detektion wird das Ereignis an das Security Information & Event Management System OSSIM weitergeleitet und dort automatisch ausgewertet. Nach Korrelation bestimmter Ereignisse erfolgt eine automatische Reaktion, die von einfacher E-Mail-Benachrichtigung des verantwortlichen Administrators oder Nutzers bis hin zur automatischen Sperrung des Internetzugangs reicht. Das CSIRT wird dabei per E-Mail entsprechend informiert und ein Ticket erzeugt. Desweiteren bietet der Anschluss an das zentrale Ticket-System die Möglichkeit, die Bearbeitung zu überwachen, um bei Bedarf auf Rückfragen von Administratoren oder Nutzern professionell reagieren zu können.

Für die Reaktion auf bestimmte Ereignisse wurde zusätzlich ein spezieller Eskalationsmechanismus entwickelt, bei dem bei erstmaliger Auffälligkeit lediglich eine Hinweis-E-Mail verschickt wird. Sollte das betreffende System oder der betreffende Nutzer nochmals auffällig werden, so erfolgt erst nach Erinnerung (frühestens nach 24 Stunden) und letztmaliger Warnung die automatische Sperrung der IP-Adresse oder Nutzerkennung. In der Praxis hat sich dieses dreistufige Vorgehen bewährt. Meist reagieren die Systemverantwortlichen bereits bei der ersten Hinweis-Meldung. Bei einigen Ereignissen, zum Beispiel bei Detektion von internen SSH-Attacken, erfolgt im Gegensatz dazu die sofortige Sperrung. OSSIM bietet an dieser Stelle durch einen policybasierten Ansatz und die Möglichkeit zur automatisierten Ausführung von Programmen genau die hierfür benötigte Flexibilität.

Kritisch zu betrachten ist die Sperrung von externen Firewall- oder Gateway-Adressen, denn dadurch sind ganze Gebäude bzw. Institute betroffen und von der Nutzung von Services im Internet abgeschnitten. Am LRZ wird deshalb eine Ausnahmenliste geführt, die sowohl für einzelne Adressen als auch ganze Subnetzbereiche verwendet werden kann. Komplette Subnetzbereiche von einer Sperrung auszunehmen ist bei Transportnetzen, NAT-Pools oder dynamisch per DHCP vergebenen Adressen notwendig. Die Benachrichtigung des CSIRTs ist auch bei einer auffälligen IP-Adresse, die als Ausnahme definiert ist, dennoch gewährleistet, um auch manuell eingreifen zu können und eine Sperrung zu forcieren.

Die Umsetzung privater in öffentliche Adressen durch den NAT-o-MAT musste bei einer automatischen Reaktion ebenfalls berücksichtigt werden. Denn eine Sperrung einer aus dem NAT-Pool dynamisch zugewiesenen Adresse ist nicht sinnvoll. Es musste ein Mechanismus entwickelt werden, der durch Auswertung von Connection Tracking Daten die zugehörige private Adresse bestimmt. Derzeit werden etwa 8800 private IP-Adressen über den NAT-o-MAT bzw. dessen Nachfolger, der sich derzeit im Aufbau befindet, geleitet. Da der Umfang des NAT-Pools beschränkt ist (zwei Class-C Netze) erfolgt die Zuordnung innerhalb weniger Sekunden auf Basis von Protokoll-, IP-Adress- und Port-Informationen.

In größeren Gebäuden ist nicht immer nur anhand der IP-Adresse der Standort des auffälligen Systems eindeutig bestimmbar. Deshalb wurde in die automatische Reaktionsskripts eine Abfrage des Tools *Nyx* [KR07] integriert. Nyx bietet die Möglichkeit, zu einer gegebenen IP- oder MAC-Adresse den Switch-Port zu detektieren, an dem das System angeschlossen ist. Diese Informationen werden den Systembetreuern automatisch mitgeliefert, um im Zweifelsfall eine rasche physische Lokalisierung des betroffenen Systems vornehmen zu können.

5.3 Manuelle, prozessorientierte Intervention

Die manuelle Meldung kann per E-Mail oder Telefon erfolgen. Nach bisheriger Erfahrung sind es meist Systemadministratoren, die nach teilweise automatisierter, toolunterstützter Auswertung von Logdaten Auffälligkeiten auf einem Server melden, die es näher zu analysieren gilt. Dazu zählen zum Beispiel Logins zu ungewöhnlichen Zeiten oder von ungewöhnlichen IP-Adressen. Manchmal werden Administratoren auch von Dienstnutzern auf ein ungewöhnliches Verhalten hingewiesen, was mitunter in direktem Zusammenhang mit einem Sicherheitsvorfall stehen kann. Demnach besteht auch die Notwendigkeit, bei einem Sicherheitsvorfall durch Einsatz einfacher Mittel Aktionen, insbesondere Analysen und Auswertungen, manuell anzustoßen.

Dazu gehören Sortier- und Filtermechanismen der zentralen SIEM-basierten Auswertungsinstanz. Nahezu auf Knopfdruck lassen sich Beginn und Zeitraum von Auffälligkeiten bestimmen. Da die Events verschiedener Monitoring-Tools parallel, zeitlich sortiert ausgewertet werden können, kann das Angriffsverhalten im Detail nachvollzogen werden. Auch zu Dokumentationszwecken leistet die integrierte Exportfunktion gute Dienste.

Daneben existieren effiziente Hilfsmittel für die einfache Konfiguration von SNORT-Signaturen. Werden z.B. verdächtige IP-Adressen in einer E-Mail-Adresse gemeldet, so bietet ein vom LRZ entwickeltes Tool, IP-Extractor, die Möglichkeit per Mausklick SNORT-Variablen zu erzeugen, die sehr komfortabel per Copy & Paste in einer IDS-Regel verwendet werden können. Dieses Werkzeug kann erweitert werden, um z.B. auch Filterregeln für NfSen im entsprechenden Format komfortabel zu erzeugen.

Das webbasierte NfSen bietet neben der manuellen Auswertbarkeit von NetFlow-Daten auch einen integrierten Alerting-Mechanismus, mithilfe dessen Administratoren in Echtzeit über die Kommunikation von bzw. zu bestimmten IP-Adressen und Ports informiert werden können. Mitarbeiter des LRZ haben desweiteren eine Reporting-Funktion implementiert, die bestimmte, per Filter reduzierte Daten in festlegbaren Intervallen automatisch auswertet und einen übersichtlichen Report erstellt, der bei Bedarf auch per E-Mail an Administratoren verschickt wird.

Auch bei notwendigem manuellem Eingriff leistet Nyx einen wichtigen Beitrag beim Auffinden von kompromittierten Systemen. Damit ist das CSIRT in der Lage, den Systemverantwortlichen vor Ort den betreffenden Switchport, an dem das System angeschlossen ist, zu nennen. Anhand dieser Informationen und meist selbsterstellter Tabellen kann das System und der zugehörige Nutzer sehr einfach und schnell identifiziert werden.

Manuell eingreifen müssen LRZ-Mitarbeiter außerdem noch bei der Freischaltung von gesperrten IP-Adressen oder Kennungen. Die Administratoren werden aufgefordert, in einer E-Mail kurz die Maßnahmen, die zur Bereinigung eines kompromittierten Systems getroffen wurden, zu schildern. Bisher funktioniert dieser Weg sehr gut. Für die Weiterentwicklung sind an dieser Stelle Automatismen wünschenswert, die die Freischaltung auf Knopfdruck, angestoßen durch den Administrator selbst, veranlassen. Dadurch könnte der zentral zu erbringende Aufwand weiter reduziert werden; aus Kundensicht würden Verzögerungen, die sich durch das Warten auf eine Reaktion auf die beschriebenen E-Mails ergeben, vermieden werden.

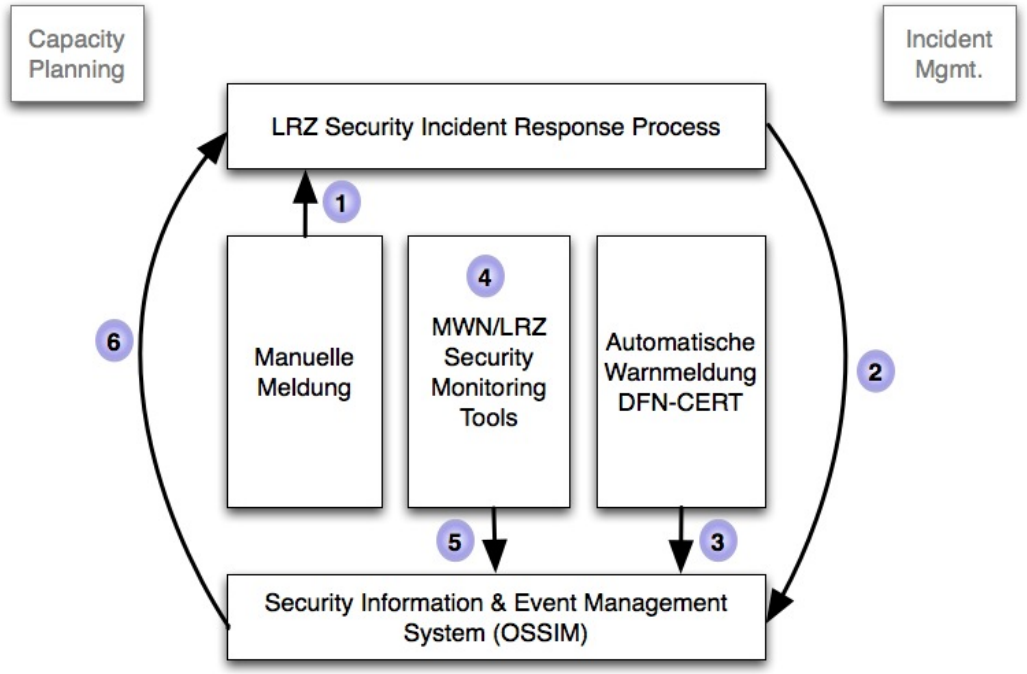

Abbildung 4: Integriertes Management von Sicherheitsvorfällen - LRZ-spezifisches Anwendungsbeispiel

5.4 Praktische Anwendung

Um zu verdeutlichen, wie das Zusammenspiel der verschiedenen Meldewege und Überwachungswerkzeuge konkret aussieht, wird an dieser Stelle noch ein kurzes Beispiel vorgestellt, bei dem die Bearbeitung wie in Abbildung 4 dargestellt abläuft: Das LRZ-CSIRT bekommt in Schritt 1 eine E-Mail von einem externen Grid-CSIRT weitergeleitet und ein entsprechendes Security-Incident Ticket im LRZ-internen Trouble-Ticket-System wird erzeugt. In der E-Mail werden eine Reihe von Details zu einem konkreten Sicherheitsvorfall, in den bereits verschiedene Grid-Knoten involviert sind, zusammengefasst. Die Meldung fordert die anderen Grid-Sites dazu auf, auf den jeweils lokalen, an die Grid-Infrastruktur angeschlossenen Systemen nach Hinweisen auf Netzverbindungen, die von bestimmten, verdächtigen IP-Adressen ausgehen, zu suchen und diese zu melden. Auf den in den Vorfall bei anderen Grid-Sites schon involvierten Knoten wurde offensichtlich der SSH-Daemon durch eine kompromittierte Version ausgetauscht. Diese erlaubt per Backdoor einen logging-freien Zugang mit Administratorrechten. Weitere Auffälligkeiten waren zum aktuellen Zeitpunkt noch nicht feststellbar.

Das LRZ-CSIRT bearbeitet den Vorfall umgehend. Bei der Klassifikation ergibt sich aus der angegebenen Quelle des Angriffs (außerhalb des MWN), dem Typ und der Anzahl der potenziell betroffenen Systeme (wenige, ausgewählte Grid-Server im LRZ) sowie der beschriebenen Art des Angriffs (root-Kompromittierung mit Austausch von Systemdateien) eine Einstufung der potenziellen Auswirkung des Angriffs im mittleren Bereich. Auf Basis der Information in der E-Mail beginnt das LRZ-CSIRT mit der Analyse der internen NetFlow-Daten (manuelle Reaktion, siehe Schritt 2). Dabei wird festgestellt, dass mehrere der gemeldeten, verdächtigen IP-Adressen mit zwei lokalen Systemen kommuniziert haben. Eine weitere Auswertung der NetFlow-Daten ergibt eine ungewöhnliche, rege Kommunikation ausgehend von diesen bei-

den Systemen in Richtung verschiedener IP-Adressen im Internet. Das LRZ-CSIRT vermutet folglich, dass diese Systeme tatsächlich kompromittiert sein könnten und informiert deshalb die zuständigen Administratoren. Als Sofortmaßnahme erfolgt, da es sich nicht um essentielle zentrale Dienste handelt, die Trennung der Netzverbindung, um jede weitere Kommunikation und damit eine mögliche Ausweitung des Vorfalls zu verhindern. Parallel dazu wird der integrierte Alerting-Mechanismus zur automatischen Auswertung der NetFlow-Daten aktiviert, um das LRZ-CSIRT bei Kommunikation der anfangs durch das Grid-CSIRT gemeldeten IP-Adressen zu informieren, um einer Kompromittierung weiterer Systeme bereits zu einem sehr frühen Zeitpunkt begegnen zu können.

Zeitgleich empfängt das LRZ-CSIRT eine automatisch generierte Meldung des DFN-CERT (Schritt 3). Darin werden ebenfalls Auffälligkeiten der zwei, dem LRZ-CSIRT bereits aufgefallenen IP-Adressen gemeldet. Diese haben versucht, bekannte Bot-Netz Control Server (C&C-Server) zu erreichen. Damit ist der Anfangsverdacht der Kompromittierung bestätigt.

Eine nun manuell durchgeführte Auswertung der IDS-Daten mithilfe des zentralen SIEM-Systems zeigt jedoch keine verdächtige Kommunikation der betroffenen Server, obwohl bestimmte Snort-Community-Regeln die Kommunikation mit aktuell bekannten C&C-Servern eigentlich überwachen sollten. Das LRZ-CSIRT entschließt sich deshalb, die vorhandenen Snort-Regeln mit einer selbstentwickelten Signatur zu erweitern (Schritt 4). Die hierfür notwendigen Informationen liefert ein Vergleich der Hinweise in den Automatischen Warnmeldungen mit den zuvor ausgewerteten NetFlow-Daten. Der integrierte Alerting- bzw. automatische Sperrmechanismus wird speziell für diese Signatur aktiviert. Damit wird bei Auffälligkeit eines weiteren lokalen Systems erreicht, dass dessen Netzverbindung automatisch getrennt wird und die zuständigen Administratoren und das LRZ-CSIRT informiert werden.

Sämtliche bis dahin vorliegenden und als relevant identifizierten Verbindungsdaten werden in einem Report zu Dokumentationszwecken exportiert; der Report wird dem Vorfallsticket als Anhang hinzugefügt. Parallel dazu wird das Grid-CSIRT über die Kompromittierung der lokalen Systeme informiert.

Die zuständigen System-Administratoren beginnen parallel dazu mit der Analyse der kompromittierten Systeme. Dabei erfolgt neben der rudimentären Auswertung der Logdaten auch die Überprüfung mit speziell für IT-forensische Analysen konzipierte Werkzeugsammlungen. Die Analyse ergibt, dass neben der ausgetauschten SSH-Daemon-Version auf den Systemen auch eine Bot-Software installiert wurde. Nach Zusammenfassen sämtlicher Details meldet das LRZ-CSIRT diese Erkenntnisse an das Grid-CSIRT weiter, welches die Beschreibung des anfangs gemeldeten Vorfalls entsprechend erweitert und an die anderen Grid-Sites weitergibt.

Zwei Tage später empfangen das LRZ-CSIRT und die zuständigen Administratoren eine E-Mail über die automatische Sperrung eines weiteren Grid-Systems im LRZ aufgrund der selbsterstellten Snort-Signatur (Schritt 5). Das betreffende System war vor einigen Tagen heruntergefahren und jetzt neu gestartet worden. Die installierte Schadsoftware wurde deshalb erst jetzt aktiv und versuchte, die selben C&C-Server zu kontaktieren. Das Vorfallsticket wird entsprechend ergänzt (Schritt 6) und die neuen Informationen werden an das Grid-CSIRT weitergeleitet. Am folgenden Tag meldete auch das DFN-CERT die Auffälligkeiten innerhalb der Automatischen Warnmeldung des zu diesem Zeitpunkt bereits vom Netz getrennten Systems, was zur Bestätigung der IDS-Signatur dient.

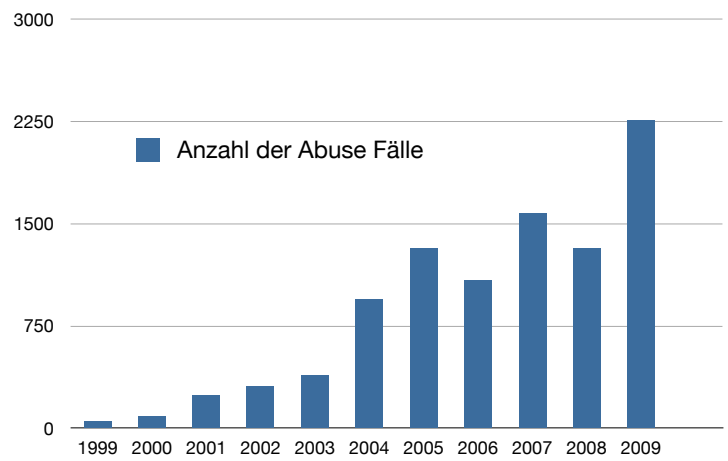

Abbildung 5: Anzahl der zu bearbeitenden Abuse-Fälle am LRZ [Böt10]

Eine weitere Kommunikation mit den anfangs als verdächtig eingestuften IP-Adressen fand nicht mehr statt. Weitere lokale Systeme sind auch nach einer definierten Beobachtungszeit von mehreren Tagen nicht mehr auffällig geworden und der Vorfall konnte abgeschlossen werden. Die gewonnenen und dokumentierten Ergebnisse werden bei der nächsten Besprechung über mögliche Verbesserungen des Security Incident Response Prozesses und der auf Grid-Systemen eingesetzten technischen Sicherheitsmaßnahmen herangezogen.

6 Zusammenfassung und Ausblick

Das Zusammenspiel von verschiedenen Meldewegen, automatisierter Auswertung und Reaktionsfähigkeit sowie die prozessorientierte Intervention sind ein effektiver und effizienter Ansatz für das integrierte Management von Sicherheitsvorfällen. Durch den hohen Grad an Automatisierung ist es möglich, trotz begrenzter Personalressourcen und auch außerhalb der normalen Geschäftszeiten zeitnah und dem jeweiligen Vorfall adäquat zu reagieren. Dass dies bitter notwendig ist, zeigt auch die in Abbildung 5 dargestellte, in den letzten Jahren massiv steigende Anzahl von Abuse-Fällen, die vom LRZ bearbeitet werden müssen. Dank der hier vorgestellten Konzepte und Werkzeuge können über 85% dieser Fälle mindestens partiell automatisiert abgewickelt und als *Standard Security Incidents* behandelt werden.

Zusammenfassend lässt sich betonen, dass für eine schnellstmögliche und strukturierte Reaktion auf sicherheitsrelevante Ereignisse die geschickte Kombination externer Meldungen, interner Monitoring-Mechanismen und interner Meldungen notwendig ist. Der Dienst Automatische Warnmeldungen des DFN-CERT leistet hierbei einen wesentlichen Beitrag und unterstützt das lokale Security-Management, indem es einerseits die Erkennung kompromittierter Systeme durch intern eingesetzte Werkzeuge bestätigt. Andererseits liefert der Dienst Anregungen zur Verbesserung der Mechanismen und bietet somit in geeigneter Weise die Möglichkeit zur Erweiterung an.

Verschiedene interne Monitoring-Mechanismen sind geeignet zu kombinieren, und die Auswertung der jeweils gemeldeten Ereignisse muss an zentraler Stelle, am besten in korrelierter Form, erfolgen. Notwendig sind außerdem vollautomatische Reaktionsmöglichkeiten, die von

einer einfachen E-Mail-Benachrichtigung bis zur Sperrung bestimmter Dienste reichen sollte. Automatismen in diesem Bereich erlauben eine Reaktion auch außerhalb der regulären Arbeitszeiten.

Zielsetzung am LRZ ist die stetige Weiterentwicklung und Verbesserung der internen Monitoring-Mechanismen und der automatischen Reaktionsfähigkeit. Die Anzahl überhaupt eintretender Sicherheitsvorfälle und damit der Umfang der automatischen Warnmeldungen des DFN-CERT müssen minimal gehalten werden. Das erklärte Ziel des LRZ ist es deshalb, die kompromittierten Systeme durch eigene Monitoring-Mechanismen frühzeitig zu erkennen und die Warnmeldung des DFN-CERT lediglich zur Bestätigung der internen Resultate heranzuziehen. Im Idealfall werden alle Sicherheitsvorfälle bereits lokal erkannt und so schnell eingedämmt, dass sie nach außen gar nicht mehr sichtbar werden.

Geplant ist ferner, dass auch noch andere, schon vorhandene Mechanismen erweitert werden. Zu diesen erweiterten Maßnahmen zählt neben der bereits durchgeführten, sofortigen Sperrung des Internet- oder MWN-Zugangs, auch die Sperrung möglichst nahe am kompromittierten System, zum Beispiel bereits am zugehörigen Switchport. Angestrebt wird auch der Aufbau eines speziellen Quarantäne-Netzes. Damit wird jede weitere Kommunikation im Münchner Wissenschaftsnetz derart eingeschränkt, dass nur ausgewählte Server (z.B. Update-Server für Betriebssysteme und Antivirus) erreichbar sind. Damit soll insbesondere der Verbreitung von Schadsoftware, ausgehend von einem kompromittierten System, innerhalb des MWN vorgebeugt werden.

In naher Zukunft wird es ein Self-Service-Portal für Administratoren geben. Darin können diese verschiedene Tätigkeiten, unter anderem die Bestimmung des Switchports mittels Nyx oder die Freischaltung gesperrter IP-Adressen, selbst vornehmen. Angedacht sind auch diverse, automatisierbare Reportingfunktionen und eine Möglichkeit, Schwellwerte für das E-Mail-Monitoring oder die Pflege der Ausnahmelisten an einer zentralen Stelle vorzunehmen. Außerdem wird die Einbettung der Scan-Ergebnisse des vom DFN-CERT seit kurzem angebotenen Netzwerkprüfers in den hier vorgestellten integrierten Ansatz angestrebt.

Literatur

[Ali10] ALIENVAULT: *Alienvault OpenSource SIEM*. `https://www.alienvault.com/products.php?section=OpenSourceSIM`, April 2010.

[Böt10] BÖTSCH, E.: *Bearbeitung von Abuse Fällen*. `http://www.lrz.de/services/security/abuse/`, Juli 2010.

[Chi10] CHICKOWSKI, ERICKA: *University Databases In the Bull's Eye*. `http://www.darkreading.com/database_security/security/attacks/showArticle.jhtml?articleID=225702686&subSection=Attacks/breaches`, Juli 2010.

[DC10] DFN-CERT: *Überblick über die Dienstleistungen des DFN-CERT*. `https://www.cert.dfn.de/`, März 2010.

[FBSR06] FLIEGL, D., T. BAUR, B. SCHMIDT und H. REISER: *Ein generisches Intrusion Prevention System mit dynamischer Bandbreitenbeschränkung*. In: MÜLLER, P.,

G. PETER und E. JESSEN (Herausgeber): *20. DFN–Arbeitstagung über Kommunikationsnetze*, Seiten 219–230, Heilbronn, Juni 2006.

[Haa05] HAAG, P.: *NfSen and NFDUMP*. http://www.terena.org/activities/tf-csirt/meeting16/nfsen-haag.pdf, September 2005.

[Hof09] HOFHERR, M. UND WIMMER, P.: *Security (Information/Event) Management - Ein Praxisbericht*. In: *16. DFN-CERT Workshop Sicherheit in vernetzten Systemen*, Hamburg, März 2009.

[Hui06] HUITEMA, C.: *Teredo: Tunneling IPv6 over UDP through Network Address Translations*. http://tools.ietf.org/search/rfc4380, Februar 2006.

[ISO05a] ISO/IEC 20000-1:2005: *Information technology — Service management — Part 1: Specification*. ISO/IEC, Geneva, Switzerland, 2005.

[ISO05b] ISO/IEC 20000-2:2005: *Information technology — Service management — Part 2: Code of practice*. ISO/IEC, Geneva, Switzerland, 2005.

[ISO05c] ISO/IEC 27001:2005: *Information technology — Security techniques — Information security management systems — Requirements*. ISO/IEC, Geneva, Switzerland, 2005.

[KR07] KORNBERGER, R. und H. REISER: *"Die Suche nach der Nadel im Heuhaufen" — Nyx — Ein System zur Lokalisierung von Rechnern in grossen Netzwerken anhand IP- oder MAC–Adressen*. In: *21. DFN Arbeitstagung über Kommunikationsnetze*, Kaiserslautern, Juni 2007.

[LR10a] LEIBNIZ-RECHENZENTRUM: *Das Münchner Wissenschaftsnetz (MWN) – Konzepte, Dienste, Infrastruktur, Management*. http://www.lrz.de/services/netz/mwn-netzkonzept/MWN-Netzkonzept-2010.pdf, April 2010.

[LR10b] LEIBNIZ-RECHENZENTRUM: *Nat-O-Mat: IP-Adressumsetzung (NAT) als Ersatz für Proxyserver*. http://www.lrz.de/services/netzdienste/nat-o-mat/, März 2010.

[MJ93] MCCANNE, S. und V. JACOBSON: *The BSD Packet Filter: A New Architecture for User-level Packet Capture*. In: *USENIX Winter*, Seiten 259–270, Januar 1993.

[oGCO07] GOVERNMENT COMMERCE (OGC), OFFICE OF: *IT Infrastructure Library v3: Service Design, 2nd impression*. ISBN 978-0113310470, The Stationery Office (TSO), 2007.

[Sou10] SOURCEFIRE: *Snort Official Documentation*. http://www.snort.org/docs, Juli 2010.