Ein Logarchiv zur Verfolgung von Sicherheitsangriffen in digitalen Vermittlungsnetzen

Sebastian Abeck, Christian Mayerl, Robert Scholderer

Universität Karlsruhe
Institut für Telematik, C&M IT Research

Tel: +49-721-608-[6391|6390] Fax: +49-721-388097
E-Mail: [abeck|mayerl]@telematik.informatik.uni-karlsruhe.de

Frank Wernert

nova data AG, D-76307 Karlsbad

Zusammenfassung

Ziel des Netz- und Systemmanagements ist der effektive und effiziente Betrieb von vernetzten Systemen. Dabei soll die gewünschte Funktionalität des vernetzten Systems mit höchster Qualität bereitgestellt werden. Ein digitales Telekommunikationsnetz als ein Beispiel für ein großes verteiltes System besteht aus einer Vielzahl von Netzknoten, von denen jeder für sich genommen bereits ein komplexes System darstellt. Der Betrieb eines digitalen Vermittlungsnetzes setzt sich aus vielen Einzeltätigkeiten an den Systemen zusammen. Die administrativen Tätigkeiten lassen sich in Logdateien aufzeichnen und bilden die Grundlage für ein Sicherheitsaudit des Betriebs. Da diese Logdaten als Massendaten an den einzelnen vermittelnden Netzknoten anfallen, muß das Zusammenziehen und Auswerten der Logdaten durch entsprechende Informatiksysteme unterstützt werden. Dieser Beitrag beschreibt den Entwurf und die Realisierung eines Logarchivs als Basis für die Verfolgung von Sicherheitsangriffen.

Schlüsselwörter:
Digitales Vermittlungsnetz, vermittelnder Netzknoten, Audit, Sicherheit, Logarchiv, Managementwerkzeuge

Computing Review Classification:
D: C.2.0, C.2.1, D.2.9, D.4.2, D.4.4, H.2.0, K.8.3, K.6.5

1 Einführung

Betreiber von vernetzten Systemen sind täglich damit konfrontiert, die Sicherheit der von ihnen angebotenen Netz- und Systemdienste zu gewährleisten, um das Vertrauen der Kunden zu bewahren. Hierzu müssen Betreiber die Sicherheit zur Aufrechterhaltung des ordnungsgemäßen Betriebs ihres vernetzten Systems fortwährend überwachen und ggf. wiederherstellen.

Unter Sicherheit wird in diesem Beitrag der Schutz vor bewußten Angriffen von Personen auf das Kommunikationsnetz und seine Komponenten verstanden. In der Literatur hat sich hierfür der Begriff `Security´ gebildet, Umwelteinflüsse bzw. zufällige Schäden gehören zum Bereich `Safety´.
Der Betreiber unterscheidet dabei einerseits externe Angreifer, die im wesentlichen Sicherheitslücken in den Telekommunikationssystemen ausnutzen und andererseits Mitarbeiter, die durch Manipulationen an den Netz- und/oder Systemkomponenten Ressourcen illegal verwenden, wie z.B. das Freischalten kostenloser Rufnummern.
Für die Sicherheit werden Online-Mechanismen, wie z.B. Paßwortschutz, Firewall und Offline-Mechanismen, die das Verhalten von Netz- und Systemkomponenten protokollieren, eingesetzt. Die Sicherheit von vernetzten Systemen wird in erster Linie durch Online-Mechanismen realisiert, die zur Laufzeit des Systems versuchen, Angriffe zu erkennen und abzuwehren. Da Online-Mechanismen niemals eine vollständige Sicherheit garantieren können, sind Möglichkeiten zur Rückverfolgung von (erfolgreichen) Angriffen auf das vernetzte System vorzusehen.

Diese Rückverfolgung stützt sich im wesentlichen auf von Offline-Mechanismen erzeugten Aufzeichnungen, die bezogen auf die Netz- und Systemkomponenten beweiskräftige Aussagen über Angriffe ermöglichen. Die Besonderheit dieser Aufzeichnungen liegt vor allem darin, daß sie die betrieblichen Abläufe, also das Verhalten des Systems einschließlich der Benutzer, widerspiegeln und somit wesentliche Informationen zum Nachweis von Angriffen beinhalten.
Eine Maßnahme zur Vermeidung vorwiegend interner Angriffe ist die Einführung eines regelmäßigen (automatisierten) Sicherheitsaudits [ISO94].

2 Infrastruktur des untersuchten Telekommunikationsnetzes

In diesem Artikel wird am Beispiel eines digitalen Vermittlungsnetzes aufgezeigt, welche technischen Voraussetzungen zur Durchführung eines solchen Sicherheitsaudits geschaffen werden müssen. Von großer Relevanz sind dabei die Logs, die von den beteiligten Komponenten während des Betriebs erzeugt werden (siehe Abbildung 1). Zur Auswertung der Logs wird ein Logarchiv benötigt, das den Offline-Mechanismen zur Aufdeckung von Sicherheitsangriffen dient.

Das digitale Vermittlungsnetz des Telekommunikationsbetreibers setzt sich aus einer großen Anzahl vermittelnder Netzknoten (VNKs) zusammen [Hals96]. Zwei Produktbeispiele von vermittelnden Netzknoten sind das EWSD-System der Firma Siemens und das S12-System von Alcatel SEL.

Der Betrieb eines VNK besteht u.a. aus dem Konfigurieren neuer Teilnehmeranschlüsse bzw. -verbindungen oder dem Einführen neuer Betriebssystemversionen usw. Das Konfigurieren wird dabei von entsprechendem Sicherheitspersonal an einem lokalen Terminal eines VNK vorgenommen. Zukünftig werden immer mehr TMN-Plattformen [Bla95, Hall96] eingesetzt, die jeweils regional zusammengefaßte VNKs verwalten. Diese Managementsysteme ermöglichen es, sich von einem entfernten Arbeitsplatz (Workstation) aus anzumelden und über die Anwendungen der TMN-Plattform die VNKs zu betreiben. Zur sicheren Übertragung der Managementinformationen werden dabei sicherheitstechnische Einrichtungen wie Lesegeräte für Chipkarten bzw. Verschlüsselungsverfahren eingesetzt. Das für den Betrieb verantwortliche Personal authentifiziert sich durch eine eindeutige Kennung. Durch die jeweilige Kennung werden entsprechend den Rollen Zugriffsrechte auf bestimmte Befehle für den Betrieb eines VNK freigeschaltet. Der (entfernte) Zugriff (über die TMN-Plattform) sowie der Betrieb eines VNK spiegelt sich in den Logdaten wider, die der VNK erzeugt. Ebenfalls entstehen Logdaten durch sicherheitstechnische Einrichtungen und die TMN-Plattform. Diese Logdaten enthalten Informationen, wer welche Aktionen zu welcher Zeit auf einem VNK durchgeführt hat. Somit spiegeln die Logdaten den Betrieb eines VNK wider und bilden die Grundlage für ein Sicherheitsaudit als ein detektives Verfahren [Sch92] zur Überprüfung des ordnungsgemäßen Betriebs der VNKs.

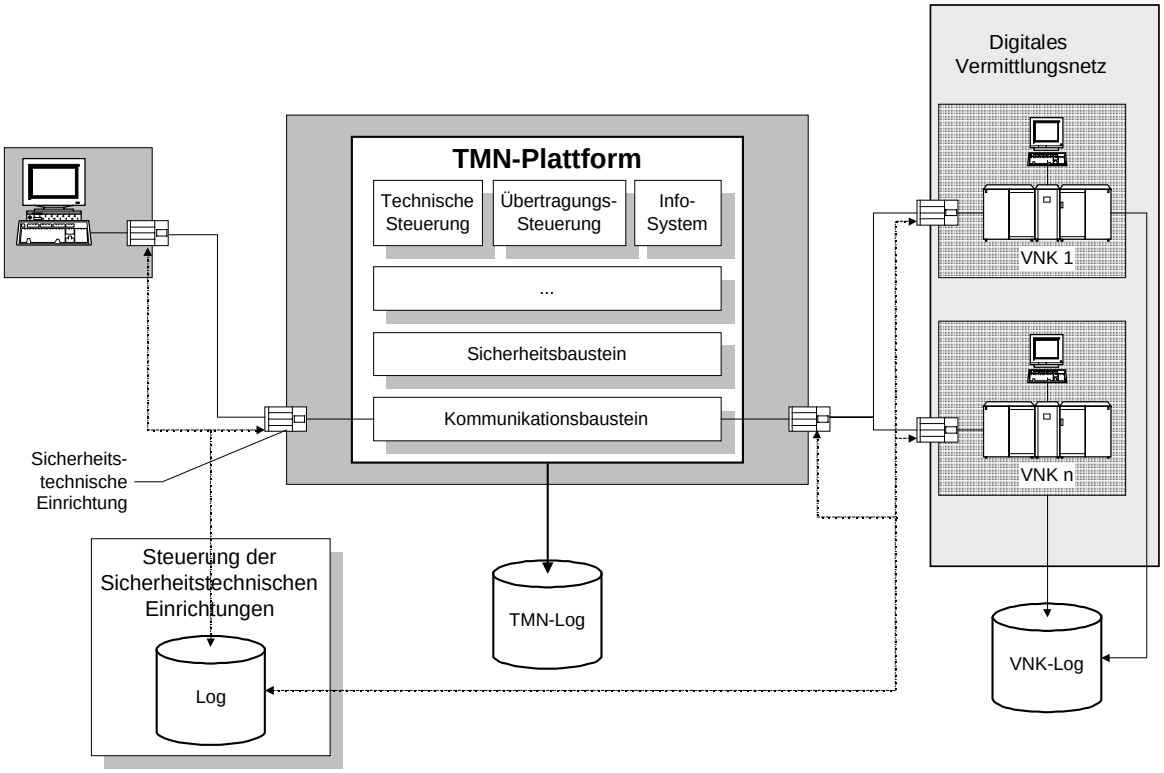

Abbildung 1: Während des Betriebs erzeugte Logs

Der Artikel zeigt die Implementierung eines Verfahrens zur systematischen Verfolgung von Sicherheitsangriffen auf das digitale Vermittlungsnetz eines Telekommunikationsbetreibers auf. Im Mittelpunkt steht dabei die Realisierung eines Logarchivs zur Auswertung und Beweissicherung der Logdaten [Ley96]. Im folgenden Abschnitt werden anhand eines Kriterienkatalogs allgemeine Anforderungen an das Logarchiv gestellt. Dabei wird stets darauf geachtet, die Anforderungen so zu gestalten, daß das Logarchiv als rechtliche Grundlage [Spi82] für eine Sicherheitsüberprüfung besteht. In einem weiteren Abschnitt werden diese Anforderungen auf das Szenario des Telekommunikationsbetreibers abgebildet und der Entwurf eines Logarchivs für das digitale Vermittlungsnetz wird aufgezeigt. In Abschnitt 5 wird das Logarchiv in ein Auditierungsverfahren bzgl. des sicheren Betriebs des digitalen Vermittlungsnetzes eingebettet. Ein Ausblick gibt den aktuellen Stand der Realisierung sowie Schwierigkeiten bei der Auswertung der Logdaten wieder.

3 Kriterien und Anforderungen an ein Logarchiv

Das Sicherheitsaudit [ISO94] stellt eine Überprüfung des ordnungsgemäßen Betriebs des digitalen Vermittlungsnetzes und seiner VNKs dar. Ziel dabei ist es, durch das Personal verursachte Unregelmäßigkeiten bei der Bedienung der VNKs zu erkennen und die Ursachen dafür zu finden. Handelt es sich um nachweislich vorsätzliche Angriffe gegen das digitale Vermittlungsnetz des Telekommunikationsbetreibers, sind weiterführende (disziplinarische) Maßnahmen einzuleiten. Aufgabe eines Logarchivs ist es, die große Menge an Logdaten als Grundlage des Audits zusammenzuführen, auf Unregelmäßigkeiten hin zu untersuchen und soweit zu verdichten, daß begründet weitere Maßnahmen angestoßen werden können. Damit die Überprüfung fundiert durchgeführt werden kann und die Beweiskraft der Logdaten sichergestellt ist, muß das Logarchiv in seiner technischen Realisierung bestimmten Anforderungen entsprechen. Nachfolgend ist eine Liste von Kriterien aufgeführt, die durch spezifische Anforderungen der jeweiligen Betreiber eines Logarchivs zu ergänzen ist:

- **Einfachheit/Wirtschaftlichkeit**
  Ein Grundprinzip bei der Überprüfung des Betriebs und dem Auffinden von Unregelmäßigkeiten ist das Prinzip der Wirtschaftlichkeit. Solange der durch evtl. Angriffe entstehende Schaden wesentlich

geringer ist als das Verfahren zur Auffindung und Verfolgung dieser Angriffe, ist die Implementierung eines derartigen Verfahrens fragwürdig. Dennoch sei vor allem auf den langfristigen Schaden hingewiesen, der sich aus immer wieder vorkommenden Einzelangriffen ergibt und somit zum Vertrauensverlust auf der Seite des Benutzers in das digitale Vermittlungsnetz und zum Imageverlust des Telekommunikationsbetreibers führt. Konkret für das Logarchiv bedeutet dies, daß die Realisierung so einfach wie möglich und so aufwendig wie nötig durchgeführt werden muß. Das Personal, das die Auswertung der Logdaten vornimmt, ist durch entsprechende Managementwerkzeuge [HeAb93] zu unterstützen, um so den Betrieb des Logarchivs effektiv und effizient zu gestalten.

- **Flexibilität/Skalierbarkeit**
  Das Logarchiv muß flexibel genug sein, um sich auf Änderungen im Betrieb des digitalen Vermittlungsnetzes einstellen zu können. Daher ist die Skalierbarkeit eine wichtige Anforderung an die technische Infrastruktur des Logarchivs, um mit einer steigenden Logdatenmenge wachsen zu können. Dabei ist nicht nur das mengenmäßige Wachstum zu berücksichtigen, sondern auch die Hinzunahme von unterschiedlich gearteten (Logdaten-)Informationen, die für das Auditierungsverfahren relevant sind und in die Auswertung einbezogen werden müssen. Des weiteren müssen das Auditpersonal sowie die Werkzeuge flexibel genug sein, so daß neu hinzukommende Angriffe in der Auswertung berücksichtigt werden können. Also muß das Logarchiv in der Lage sein zu lernen.
- **Gerechtigkeit**
  Aufgabe des Logarchivs ist das Auffinden von Unregelmäßigkeiten im Betrieb der VNKs. Dabei kann eine auffällige Abweichung vom Normalbetrieb in Ausnahmefällen gerechtfertigt sein. Das Logarchiv stellt die Grundlage für nachfolgende Maßnahmen wie die Rechtfertigung dieser Unregelmäßigkeit dar. Dabei sollte darauf geachtet werden, daß aufgrund einer mangelhaften Auswertung nicht ständig unbegründete Verdächtigungen ausgesprochen werden. Das Logarchiv muß über das Ergebnis der weitergehenden Nachforschungen von Unregelmäßigkeiten informiert werden, um den Lernprozeß zu unterstützen und so die Trefferwahrscheinlichkeit der Auswertung zu erhöhen. Oberstes Ziel des Sicherheitsaudits ist es, niemanden aufgrund der Überprüfung zu Unrecht eines Angriffs zu beschuldigen.
- **Zuverlässigkeit/Korrektheit**
  Die Auswertung und Archivierung der Logdaten muß zuverlässig und korrekt sein, damit eine ordentliche Durchführung des Auditierungsverfahrens und damit die Beweiskraft sichergestellt ist. Die technischen Systeme und Werkzeuge müssen stabil laufen, ohne den Betrieb des Logarchivs ständig zu stören und damit die Durchführung des Sicherheitsaudits zu behindern. Die einzusetzenden, automatisierten Werkzeuge zur Datenübertragung, Archivierung und Auswertung dürfen den Informationsinhalt der Logdaten weder verändern noch fehlerhaft interpretieren. Treten Unschärfen bei der Auswertung der Information auf, muß man sich dieser bewußt sein, um das Ergebnis der Auswertung entsprechend beurteilen zu können.
- **Vollständigkeit**
  Das Ziel des Logarchives und des Auditierungsverfahrens besteht im Auffinden von allen Unregelmäßigkeiten im Betrieb des digitalen Vermittlungsnetzes. Um diesem Ziel möglichst nahe zu kommen, ist es notwendig, alle Logdaten vollständig in das Logarchiv zu übertragen und auszuwerten. Dazu können ergänzende Zusatzinformationen notwendig sein, um die Massendaten korrelieren und Schlußfolgerungen ziehen zu können. Dennoch ist durch die Untersuchung aller Logdaten noch nicht gewährleistet, daß jeder Angriff gefunden wird. Aber die Wahrscheinlichkeit, daß die durch einen Angreifer verursachten Unregelmäßigkeiten bei der Auswertung erkannt werden, werden aufgrund der Erfahrungsgewinnung immer größer. Die Vollständigkeit des Logarchivs erhöht zudem präventiv die Hemmschwelle zur Durchführung von Manipulationen.
- **Sicherheit**
  Das Logarchiv und seine technische Infrastruktur selbst kann wiederum zu einem Ziel von Angriffen werden. Damit eine korrekte Auswertung und Beweissicherung garantiert werden kann, muß das Logarchiv und der gesamte Auditierungsprozeß gesichert werden. Angriffspunkte sind dabei vor allem die Übertragungswege der Logdaten, das Archivierungssystem sowie die Auditoren, die mit

Hilfe von (automatisierten) Werkzeugen die Auswertung vornehmen. Durch den Ausfall einzelner Komponenten im Logarchiv darf das gesamte Auditierungsverfahren nicht zum Erliegen kommen. Die Funktionalität und Verfügbarkeit des Logarchivs muß entsprechend stabil sein und durch hinreichende Notfallkonzepte [BHG87] abgesichert sein.

- **Datenschutz**
  Ein wichtiger Aspekt für die Implementierung und Akzeptanz des Sicherheitsaudits in der Praxis ist die Gewährleistung des Datenschutzes [Wäh93]. Ein Kritikpunkt ist dabei die Möglichkeit der totalen Überwachung des Bedienpersonals. Durch entsprechende Automatisierung und Anonymisierung kann die jeweilige Bedienperson bei der routinemäßigen Überprüfung geschützt werden. Erst bei begründetem Verdacht ist eine Abbildung auf die Personaldaten notwendig. Durch entsprechend technische und betriebliche Vorkehrungen muß innerhalb des Logarchivs dafür gesorgt werden, daß mit diesen Informationen kein Mißbrauch getrieben wird. Dies kann z.B. dadurch geschehen, daß durch technische Einschränkungen kritische Informationen nur unter dem Vier-Augen-Prinzip bearbeitet werden können.

Dies ist eine Auswahl von allgemeinen Anforderungen, die ein Logarchiv erfüllen sollte, um als fundierte Grundlage für ein Sicherheitsaudit zu bestehen. Weitere und detailliertere Anforderungen sind stark vom jeweiligen Betreiber abhängig. Im folgenden wird am Beispiel eines Telekommunikationsbetreibers der Entwurf und die Realisierung eines Logarchivs unter der Berücksichtigung der oben genannten Anforderungen vorgestellt.

4 Entwurf des Logarchivs für ein digitales Vermittlungsnetz

Das Logarchiv nimmt eine zentrale Stellung bei der Überprüfung des Betriebs ein. Die zu erfüllende Aufgabe ist in erster Linie die Auswertung der Logdaten. Um weiterführende Maßnahmen bzgl. eines Angriffs durchführen zu können, müssen die Logdaten im Sinne eines Beweismittels archiviert werden. Damit die gestellten Aufgaben erfüllt werden können, besteht die Architektur des Logarchivs aus entsprechenden konzeptionellen Bausteinen. Aufgrund der hohen Sicherheits- und Leistungsanforderungen an das Logarchiv, ist die Abbildung dieser Bausteine auf konkrete Software- und Hardwaresysteme ein Kernpunkt des Entwurfs des Logarchivs.

4.1 Architektur des Logarchivs

Die Gesamtfunktion des Logarchivs wird durch die Kooperation der einzelnen (Teil-)Bausteine erbracht. Abbildung 2 zeigt diese Bausteine und deren Beziehungen zueinander.

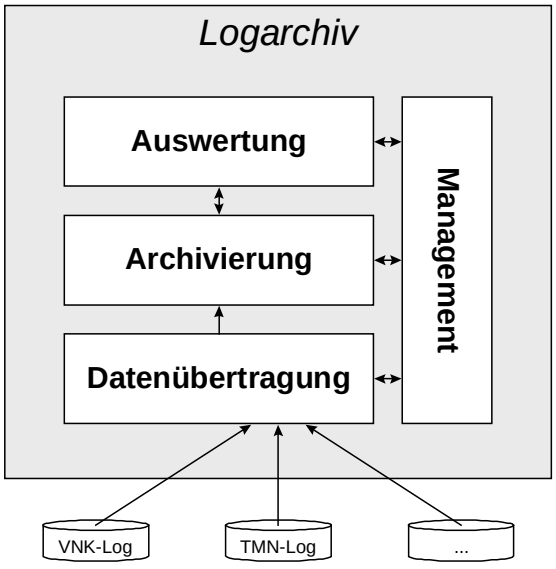

Abbildung 2: Bausteine des Logarchivs

Die Komponenten des digitalen Vermittlungsnetzes sind geographisch verteilt. Aufgabe der Datenübertragung ist das Zusammenziehen der verteilt anfallenden Logdaten in das Logarchiv. Ein Problem ist dabei die große Menge der Logdaten, d.h. pro Vermittlungsknoten 6 MegaByte Logdaten an; dies entspricht bei 1800 VNKs einem täglichen Gesamtdatenaufkommen von ca. 11 GigaByte. Die Verwaltung der Logdaten im Sinne einer Dateiverwaltung oder eines Datenbanksystems wird durch die Archivierung durchgeführt. Auf die Archivierung schließlich setzt die Auswertung der Logdaten auf. Dabei werden die angelieferten „rohen“ Logdaten analysiert und auf eventuelle Unregelmäßigkeiten hin untersucht. Bereits gewonnene Informationen werden ebenfalls archiviert. Im Hinblick auf einen effektiven und effizienten Betrieb des Logarchivs wird eine Migration hin zu einem möglichst hohen Grad der Automatisierung der Logverarbeitung angestrebt. Ein entsprechendes Managementsystem unterstützt dabei die Kontrolle und Steuerung der einzelnen Bausteine.

4.1.1 Datenübertragung

Die Datenübertragung stellt die Verbindung zwischen den Erzeugersystemen der Logdaten und dem Logarchiv dar. Die Datenübertragungskomponente initiiert mindestens täglich die Übertragung der angefallenen Informationen aller Logquellen, überwacht den Übertragungsvorgang und übergibt die korrekt empfangenen Daten an die Archivierungskomponente. Eine tägliche Abfrage ist insbesondere erforderlich, da die Dateien, die die Log-Informationen enthalten, bei Vermittlungsknoten eine Füllgröße von 40MB aufweisen und beim Überlauf die protokollierte Information zyklisch überschreiben.
Die Datenübertragungskomponente muß so dimensioniert sein, daß selbst bei länger andauernder Spitzenbelastung keine Pufferüberläufe und Datenverluste auftreten können [PGK87]. Weiterhin muß die eingangsseitige interne Bandbreite hoch genug sein, um die Logdaten innerhalb eines Zeithorizonts von wenigen Stunden in das Archiv einbringen zu können. Das Zeitfenster im vorliegenden Szenario liegt bei ca. drei Stunden; innerhalb dieser Zeit müssen alle Log-Informationen von den Logquellen übertragen sein. Die verbleibenden Stunden sind für Übertragungen weiterer Informationen (z.B. Abrechnungsdaten) und den Routinebetrieb reserviert. In dieser Komponente können bereits Meta-Daten über die einzelnen Logdaten erzeugt und ebenfalls der Archivierung übergeben werden.

4.1.2 Archivierung

Die Archivierung nimmt die Logdaten entgegen und speichert diese auf einem persistenten Speichermedium. Der Speicherbereich, der die täglichen Daten aufnimmt, heißt Tagesdatenbasis. Die Auswertung der täglich anfallenden Logdaten setzt auf der Tagesdatenbasis auf. Nach der Auswertung migrieren die Tagesdaten in die History-Datenbasis. Um ein effizientes und möglichst transparentes Handling des Archivierungssytems zu ermöglichen, ist eine Verwaltung der archivierten Logdaten und Meta-Daten erforderlich. Diese Verwaltung bildet die Schnittstelle zwischen Auswertung und Archivierung. Bei der Dimensionierung der Speichermedien steht der benötigte Durchsatz zur Übernahme der Daten von der Datenübertragung im Vordergrund, da es hier zu keinen Datenstaus kommen darf. Die Geschwindigkeit der eingesetzten Speichermedien bildet eine weitere Kenngröße. Die Tagesdatenbasis muß über einen wahlfreien schnellen Zugriff verfügen, die History-Datenbasis kann auf langsameren und kostengünstigeren Speichermedien plaziert sein, da die Migration der Daten von der Tages- in die History-Datenbasis zu Zeiten der Minderbelastung geschehen kann.

4.1.3 Auswertung

Die Auswertung übernimmt die eigentliche Erkennung von Angriffen auf die Logquellen. Unter der Prämisse, daß die Logdaten grundsätzlich eine Erkennung von Angriffen ermöglichen, werden die Logdaten nach Angriffen durchsucht. Die Inspektion kann manuell oder automatisch erfolgen. Dabei bildet die manuelle Inspektion die Grundlage der automatischen Inspektion. Bei der manuellen Inspektion greift der Auditor über das Archivierungssystem und die dort vorliegenden Meta-Daten auf eine Logdatei zu und durchsucht diese mittels geeigneter Werkzeuge. Die dabei gewonnenen Erkenntnisse über die Erkennung bestimmter Angriffe werden in die automatische Logauswertung eingebracht. Eine effiziente und effektive Auswertung setzt Wissen über die Semantik der Logdaten voraus. Werden Logdateien ausgewertet, deren Struktur und damit Semantik nicht bekannt sind, liegt vor der manuellen Auswertung ein Prozeß der Wissensgewinnung [Bol96] über den Aufbau der

Logdatei. Wurde die Struktur analysiert, bleibt auch diese typbezogene Strukturinformation im Archiv erhalten. Besteht die Möglichkeit, auf die Struktur der Logdaten Einfluß zu nehmen, sollte auf deren konsistente und einfach auszuwertende Beschreibung (z.B. in ASN.1) besonders großen Wert gelegt werden, da die Qualität der Auswertung von der Qualität der Logdaten unmittelbar abhängt.

4.1.4 Management

Das Management dient der Kommunikation und Koordination der Bausteine untereinander. Des weiteren überwacht es die Übertragung der Logdaten und die Übergabe der Logdaten von der Datenübertragung an die Archivierung. Es stellt im Fehlerfall geeignete Fehlerbehandlungsmechanismen zur Verfügung oder propagiert den Fehler bis zum Bedienpersonal des Logarchivs, das dann entsprechende Maßnahmen ergreift. Grundsätzlich bildet das Management das Rückgrat des Logarchivs, da es das Zusammenspiel der einzelnen Bausteine realisiert. Bei der Realisierung der Management-Komponente wird besonderer Wert auf Fehlertoleranz und Zuverlässigkeit gelegt.

4.2 Realisierung einer zentralisierten Verarbeitungsinfrastruktur

Die Realisierung des Logarchivs führt zu einer Abbildung der konzeptionellen Bausteine auf konkrete Software- und Hardwaresysteme. Dabei können mehrere Bausteine auf einem System etabliert oder ein Baustein kann durch mehrere Systeme realisiert sein. Grundsätzlich müssen die einzelnen Bausteine demnach nicht an einer zentralen Stelle liegen, sondern können regional verteilt auf lose gekoppelten Systemen organisiert sein. Demzufolge ist sowohl eine zentrale, eine regional verteilte oder eine hierarchische Realisierung möglich. Eine Auswertung stellt jedoch bestimmte Bedingungen an das Logarchiv:

- Die Logdaten sollen ohne Zwischenlagerung an das Logarchiv übertragen werden, um die Möglichkeit der Manipulation zu verringern.
- Logdaten verschiedener Quellen müssen miteinander konsolidiert werden, um den Weg, den ein Angreifer genommen hat, nachvollziehen zu können (User Tracing, [May95]).
- Zur Beweissicherung müssen die Logdaten eine bestimmte Zeit aufbewahrt werden.

Im folgenden wird die Realisierung einer zentralen Verarbeitungsinfrastruktur aus der Perspektive des Telekommunikationsbetreibers betrachtet. Die alternativen Ansätze (regional verteilt, hierarchisch) sind in der Realisierung mit einem hohen Aufwand durch zusätzliche Hard- und Softwarekomponenten an allen Vermittlungsknoten verbunden. Des weiteren enthalten diese Ansätze zu viele Sicherheitsprobleme, wie der nicht kontrollierbare Zugriff auf benutzerspezifische Logdaten über einen beliebigen Zeitraum hinweg. Aus diesen Gründen wird im weiteren nur die zentralisierte Variante verfolgt.
Eine zentralisierte Verarbeitungsinfrastruktur hat gegenüber der verteilten sowohl Vorteile als auch Nachteile. Nachteilig ist die Notwendigkeit einer Übertragung aller Dateien an die Zentrale. Diese Vorgehensweise setzt eine hohe Kapazität der Datenübertragungskomponente des Logarchivs voraus. Die administrativen Tätigkeiten zur Installation und Wartung dieser Komponente sind gegenüber einer lokalen Auswertung am VNK vor Ort sehr aufwendig. Um die notwendige Bandbreite zu gewährleisten, muß gegebenenfalls eine hohe Parallelität realisiert werden. Die Verfügbarkeit des Systems muß, da die Logdaten lückenlos archiviert werden, bei 100 Prozent liegen. Das kann durch geeignete Hardware-Redundanz erreicht werden. Welche Hardware-Komponenten im einzelnen notwendig sind, ist mit den entsprechenden Herstellern abzuklären. Die Vorteile einer Verarbeitungsinfrastruktur mit zentralem Charakter sind die vereinfachte Administration und die vollständig verfügbare Information aller Logdaten. Liegt die gesamte Verarbeitungsfunktionalität geschlossen vor, sind Änderungen an der Auswertungsfunktionalität mit relativ wenig Aufwand durchzuführen. Die Planung und Durchführung obliegt dem zuständigen Systemadministrator. Absprachen mit Systemadministratoren anderer Systeme sind nicht notwendig, da Änderungen für die Logquellen transparent sind. Die Logquellen produzieren die Logdaten wie bisher, die Art und Weise der Verarbeitung der Daten in der Zentrale hat darauf keine Auswirkungen. Die durch die Zentralisierung gewährleistete Verfügbarkeit aller Logdaten ist für die effiziente Auswertung notwendig. Die Erkennung von Angriffen und deren Zurückverfolgung auf den Verursacher benötigen unter Umständen Logdaten verschiedener Logquellen. Da alle Logdaten in der Zentrale vorliegen, kann eine Konsolidierung von Logdaten verschiedener Logquellen durchgeführt

werden. Zur Beweissicherung und nachträglichen Inspektion sind alle Logdaten für die Dauer mindestens eines Jahres zu archivieren. Alle Daten, die zur Auswertung in das zentrale Logarchiv übertragen werden, müssen auch archiviert werden. Das Archivsystem des Logarchivs muß allen Anforderungen an moderne Datenbanksysteme entsprechen. Um eine lückenlose, fehlerfreie und permanente Archivierung zu jeder Zeit zu gewährleisten, muß eine entsprechende Hard- und Software-Redundanz auf der Archiv-Ebene möglich sein.

4.3 Gesamtfunktionalität

Die Gesamtfunktionalität des Zentralen Logarchivs ist in verschiedene Funktionseinheiten aufgeteilt, wie Abbildung 3 im Überblick zeigt.

- Die Logempfangseinheiten nehmen die Daten entgegen, der Archivrechner archiviert die Logdaten dauerhaft und stellt Dienste für den Zugriff zur Verfügung. Auswertungsrechner stellen die Funktionalität der Auswertungswerkzeuge zur manuellen und automatischen Auswertung der Logdateien bereit.

  Dieser Funktionsumfang stellt jedoch nur die Lösungen für jeweils kleine, abgegrenzte Teilgebiete bei der Verarbeitung der Logdaten dar. Eine integrierte Gesamtverarbeitung ist damit jedoch nicht zu erzielen. Ein übergeordnetes System verwaltet die einzelnen Teilschritte intelligent und effizient.

  Ziel der Administration ist eine integrierte Verarbeitung aller Teilprozesse des Zentralen Logarchivs. Die Teilprozesse leisten jeweils einen kleinen Teil des Verarbeitungsvorgangs der Logdaten. Diese Teilprozesse müssen jedoch organisiert werden. Die Organisation der Verarbeitung umfaßt Aktionen wie Koordination, Kooperation, Kommunikation, Überwachung oder Ausnahmebehandlung. Diese Aktionen bedingen sich meist gegenseitig und werden im folgenden Teil kurz eingeführt.

- Die Koordination [Wer94] der einzelnen Prozesse, die im Zentralen Logarchiv abgearbeitet werden, ist zwingend erforderlich. Koordination ist die Abstimmung mehrerer Vorgänge, die entweder parallel oder seriell abgewickelt werden sollen. Beispiele von Koordinationen im Rahmen der Verarbeitungstätigkeit ist die Übergabe einer Logdatei nach der Übertragung an das Archiv und die Übergabe einer übertragenen Datei an die automatische Logauswertung. Letzteres Beispiel wird im folgenden Abschnitt exemplarisch dargestellt.

- Unter Kooperation versteht man das gemeinsame Zusammenwirken mehrerer Beteiligter, um ein gemeinsames Ziel zu erreichen, das ein Einzelner nicht oder nur sehr langsam erreichen würde. Eine Kooperation im Sinne der Verarbeitung ist die gemeinsame Empfangstätigkeit mehrerer Logempfangseinheiten, die zusammen die Datenübertragungskomponente des Zentralen Logarchivs darstellen. Eine Logempfangseinheit alleine wäre nicht in der Lage, die Logdateien aller Logquellen innerhalb des vorgegebenen Zeitraums entgegenzunehmen.

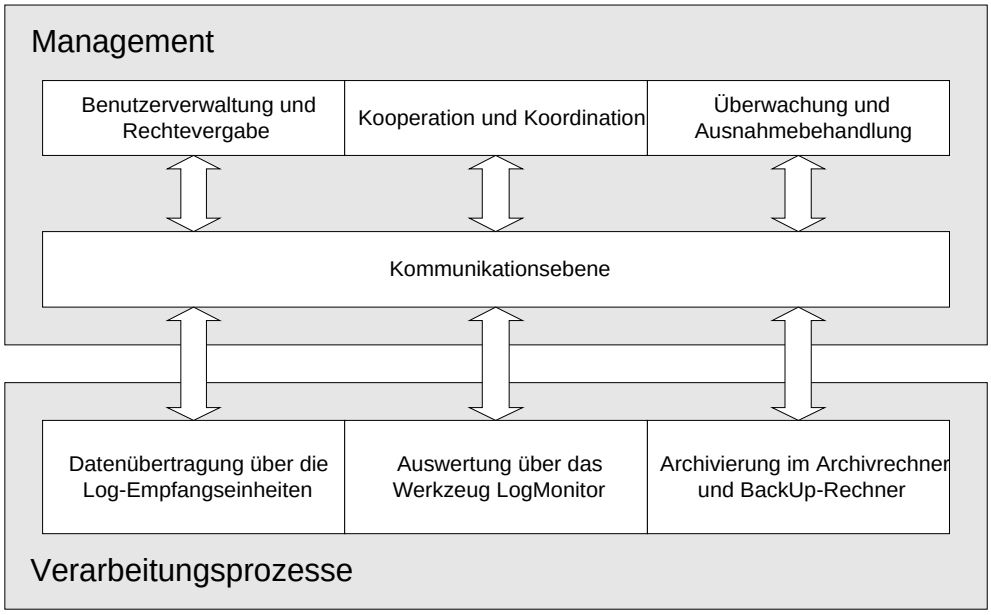

Abbildung 3: Das Administrationssystem im Zentralen Logarchiv

- Die Kommunikation innerhalb des Zentralen Logarchivs spielt eine wesentliche Rolle. Kommunikationsparadigmen, wie die Signalisierung oder die Benachrichtigung ermöglichen den Austausch von Informationen zwischen den einzelnen Teilprozessen. Ohne geeignete Kommunikation könnte eine Koordination von Prozessen nicht stattfinden; z.B. erhalten Prozesse zur Archivierung vom Übertragungsprozeß die Information, daß die Übertragung beendet ist und das Ergebnis (die Logdatei) zur Weiterverarbeitung bereit steht.

  Die Administration des derart komplexen Systems Zentrales Logarchiv kann durch entsprechend konfigurierte Software realisiert werden. Eine Möglichkeit bietet der Einsatz von Management Plattformen, wie z.B. HP OpenView.

5 Einbettung des Logarchivs in das Auditierungsverfahren

Das aufgezeigte Logarchiv steht im Mittelpunkt eines zu implementierenden `Security Audit Cycle´ ([GMITS]). Gegenstand dieses Audits ist der Betrieb des digitalen Vermittlungsnetzes. Mit Hilfe dieses Verfahrens werden kurzfristig *Angriffe* von internen Mitarbeitern erkannt sowie langfristig der Betrieb im Hinblick auf ordnungsgemäße Bedienung überwacht und sichergestellt. Der Prozeß der Auditierung [GrMa91] definiert dabei die Rolle sogenannter Auditoren. Als Team im Logarchiv zusammengefaßt werden diese Rollen durch ausgewählte Mitarbeiter der Betreiberorganisation besetzt. Man spricht dabei von einem (Unternehmens-)internen Audit im Gegensatz zu einem externen Audit durch Beauftragung einer unternehmensfremden Beratungsfirma.

5.1 Auditierungsverfahren

Ein Audit ist eine Methode des Managements zur Überprüfung und Verbesserung von komplexen Systemen (vgl. [GrMa91, GMITS, CCT94, SCH92]). Das Verfahren basiert dabei meist auf der Auswertung von Massendaten, die geeignet verdichtet werden müssen, um präzise Aussagen treffen zu können. Abbildung 4 zeigt die zyklische Abfolge der drei Phasen eines Audits.

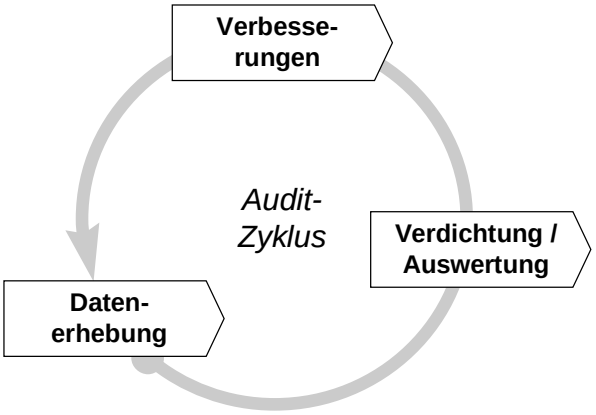

Abbildung 4: Zyklisches Auditierungsverfahren

In der ersten Phase werden relevante Daten erhoben, die zur Überprüfung herangezogen werden. Die Eigenschaften der erhobenen Daten bestimmen die Effektivität des Audits, d.h. je umfangreicher und aussagekräftiger die erhobenen Daten sind, desto genauer ist das Auswertungsergebnis dieser Daten. Das Ergebnis der Auswertung kann nur so gut sein, wie die zur Auswertung herangezogenen Daten. Daher ist die Phase der Datenerhebung durch eine Vielzahl und Vielfalt von Daten geprägt. Damit das Management Entscheidungen treffen kann, ist es notwendig, diese Massendaten in der zweiten Phase zu verdichten und zu präzisen Aussagen auszuwerten. Die Methodik und der Grad der Automatisierung der zweiten Phase bestimmen u.a. die Effizienz des Auditierungsverfahrens. In einer dritten Phase werden Maßnahmen zur Verbesserung durchgeführt. Zum einen betreffen diese Verbesserungen den Gegenstand der Überprüfung; im vorliegenden Szenario ist dies der Betrieb des digitalen Vermittlungsnetzes. Zum anderen wird die Datenerhebung und Auswertung verbessert, um die Ergebnisse des Auditverfahrens immer präziser zu fassen. Das Auditierungsverfahren ist aufgrund seiner zyklischen Abfolge in der Lage, zu lernen und sich auf neue Situationen einzustellen.

5.2 Sicherheitsaudit bei einem Telekommunikationsbetreiber

Ziel des Telekommunikationsbetreibers ist es, ein Auditierungsverfahren zu implementieren, das die Sicherheit des digitalen Vermittlungsnetzes überwacht und verbessert. Kurzfristig werden dabei *Angriffe* gefunden und verfolgt. Langfristig wird das Bewußtsein der Mitarbeiter sich dahingehend verändern, daß derartige Manipulationen im digitalen Vermittlungsnetz dem Unternehmen und damit dem eigenen Arbeitsplatz schaden. Damit ein derartiger Auditprozeß realisiert werden kann, sind Maßnahmen sowohl bzgl. der Ablauforganisation als auch der Aufbauorganisation vorzunehmen. Zudem ist dieser Prozeß durch entsprechende Managementwerkzeuge zu unterstützen, um die Durchführung möglichst effektiv und effizient zu gestalten.

5.2.1 Ablauforganisation

Ausgehend von einer groben Prozeßbeschreibung, wie sie in Abbildung 5 zu sehen ist, werden die durchzuführenden Tätigkeiten detailliert spezifiziert und zueinander in Beziehung gesetzt. Dabei sind bereits bestehende Verfahren und Gewohnheiten innerhalb des Unternehmens als Randbedingungen zu berücksichtigen. Abbildung 5 zeigt eine derartige grobe Prozeßmodellierung.

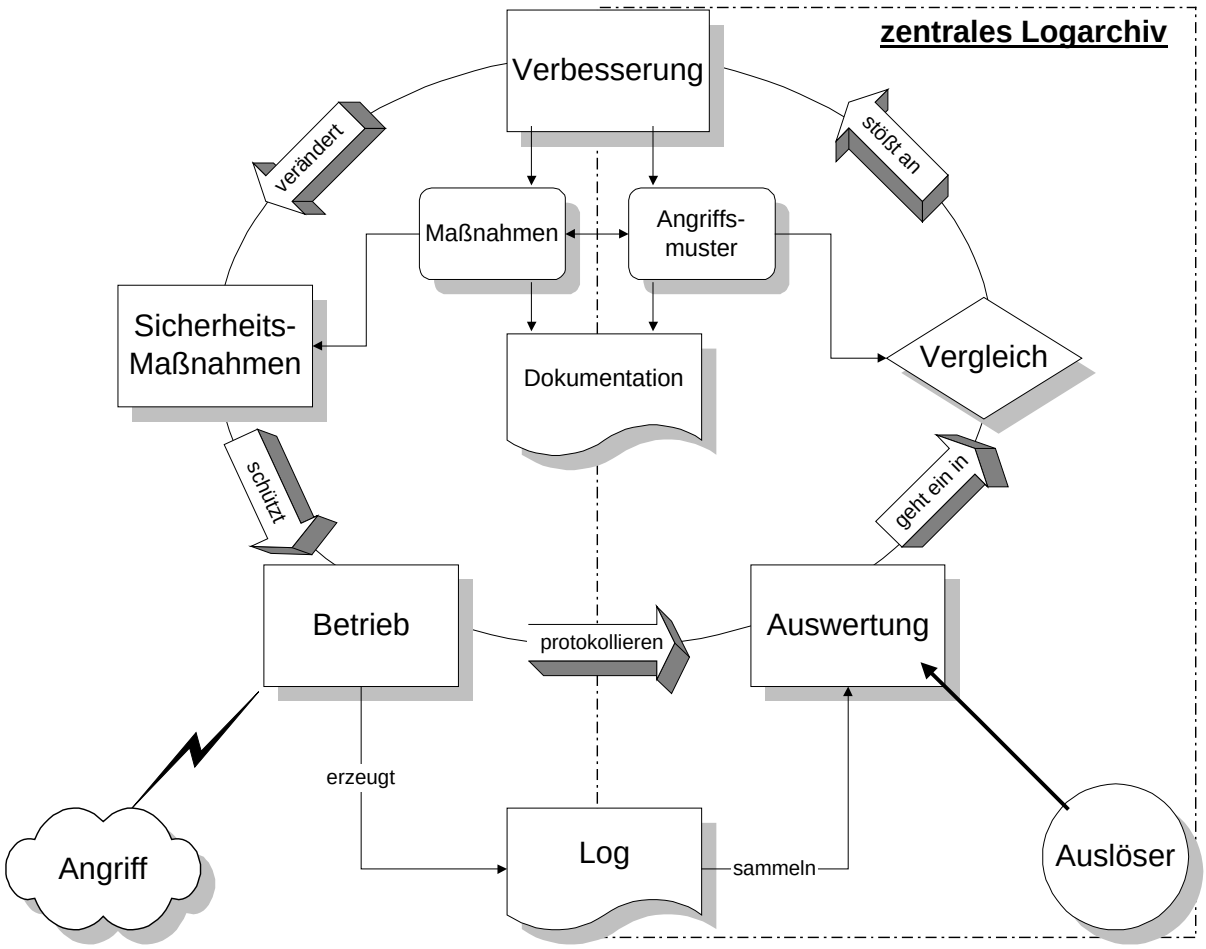

Abbildung 5: Sicherheitsaudit bei einem Telekommunikationsbetreiber

Während der Bedienung der VNKs fallen eine große Anzahl von Logdaten an. Die Logdaten protokollieren den Betrieb des digitalen Vermittlungsnetzes. Findet ein Angriff durch das Bedienpersonal in Form einer unrechtmäßigen Manipulation statt, wird dies in den Logdaten festgehalten. Da sich die Angriffsmuster über mehrere Logdaten erstrecken können, ist es notwendig, die Logdaten im Logarchiv zusammenzuziehen. Die Auswertung verlangt zudem die Möglichkeit, unterschiedliche (Logdaten-)Informationen zu konsolidieren, z.B. über mehrere, regional verteilte VNKs oder über TMN-, VNK-Logdaten und Logdaten der sicherheitstechnischen Einrichtungen hinweg. Die Auswertung kann dabei stichprobenartig oder möglichst kontinuierlich (automatisiert) erfolgen. Wesentliche Aufgabe innerhalb der Auswertung ist das Auffinden von *Angriffsmustern*, die durch Erfahrung gelernt und entsprechend dokumentiert werden. Die Auffindung von nachweisbaren Angriffen stößt zweierlei Verbesserungsmaßnahmen an. Zum einen werden Maßnahmen durchgeführt, die direkt den Betrieb der VNKs sicherer gestalten. Dies können Änderungen in den Systemen oder auch auf personeller Ebene sein. Zum anderen werden Maßnahmen zur Verbesserung des Audit-Zyklus selbst durchgeführt. Es werden Erfolge dokumentiert, um auf die Erfahrungen zurückgreifen zu können. Zudem wird relevantes Zusatzwissen identifiziert, durch dessen Hinzunahme die Auswertung effektiver und effizienter wird. Aufgrund der Dynamik der Angriffsmuster werden stets neue Muster erkannt und dokumentiert. D.h., der Auditprozeß ist in der Lage, sich an neue Gegebenheiten anzupassen, er lernt.

5.2.2 Aufbauorganisation

Des weiteren definiert der Auditprozeß Rollen, die bestimmte Aufgaben zu erfüllen haben und in der Organisation verankert sein müssen. Das Personal des Logarchivs nimmt dabei die Rolle von internen Auditoren ein. Dabei müssen die Aufgaben und Verantwortungsbereiche entsprechend den Funktionen im Logarchiv auf das Personal verteilt werden. Entsprechend qualifiziertes und autorisiertes Personal ist mit der Auswertung der Logdaten zu beauftragen. Eine weitere Rolle innerhalb der Auditgruppe ist der

Datenschutzbeauftragte, der die Auswertung entsprechend den Datenschutzvorschriften überwacht. Des weiteren ist ein enger Kontakt mit den Herstellern bzw. dem Betriebspersonal zu pflegen. Bei Änderungen in der Bedienung z.B. durch Hinzunahme von neuen Befehlen sind die Auditoren davon in Kenntnis zu setzen. Um weiterführende Maßnahmen anstoßen zu können und Auskunft über das Ergebnis einer Maßnahme zu garantieren, ist die Kooperation mit den entsprechenden Rollen zu pflegen.

6 Ausblick

Ein offensichtliches Problem bei der Realisierung des Logarchivs ist die Menge der Logdaten, die übertragen und ausgewertet werden muß. Dieses Problem ist nur durch einen hohen Grad an Parallelisierung und durch leistungsfähige Systeme lösbar. Folglich entstehen sehr hohe Investitionskosten. Um die Kosten zeitlich zu verteilen, wird die Realisierung schrittweise durchgeführt. In der ersten Projektphase werden Systeme eingesetzt, die den Minimalanforderungen des Logarchivs entsprechen. Wichtigste Randbedingung ist dabei aber stets, daß diese Systeme skalierbar in Richtung Vollfunktionalität des Logarchivs sind.

Eine besondere Herausforderung im Zusammenhang mit dem Logarchiv stellt die Gewinnung geeigneter Angriffsmuster dar. Bislang befindet sich das Wissen, wann ein durch entsprechende Logdaten beschriebener Vorgang im digitalen Vermittlungsnetz auf einen Angriff hindeutet, in den Köpfen der Experten. Dieses Wissen in Form von Anfgriffsmustern explizit auszudrücken und damit die Auswertung durch geeignete Analysewerkzeuge rechnergestützt ablaufen zu lassen, ist eines unserer momentan bearbeiteten Hauptziele. Hierbei kommt dem beschriebenen Log-Monitor, der bereits erfolgreich im Einsatz ist, eine große Bedeutung zu.

In diesem Beitrag wurde ein Verfahren aufgezeigt, das die Überprüfung des digitalen Vermittlungsnetzes eines Telekommunikationsbetreibers basierend auf unterschiedlichen Logdaten erlaubt. Eine Eigenschaft der Logdaten ist, daß sie einen wesentlichen Teil der Betriebsprozesse am VNK widerspiegeln. Folglich erlauben die Logdaten nicht nur eine Überwachung der Betriebsprozesse bzgl. der Sicherheit, sondern z.B. auch bzgl. einer effizienten Bedienung der VNKs. Das Logarchiv bietet die Möglichkeit, das Auditverfahren dahingehend zu erweitern.

7 Literaturverzeichnis

[Abe96] Sebastian Abeck: Integrated Resource Management: A Process-Oriented Approach, European Summer School of ‘European Network of Universities and Companies in Information and Communication Technologies´ (Eunice´96), Lausanne, September 1996.

[BHG87] Philip A. Bernstein, Vassos Hadzilacos, Nathan Goodman: Concurrency control and recovery in database systems, Addison-Wesley, 1987.

[Bla95] Uyless D. Black: Network management standards: SNMP, CMIP, TMN, MIBs, and Object Libraries, McGraw-Hill, 1995.

[Bol96] Georg Bol: Wissensgewinnung aus großen Datenbasen: Seminar im Wintersemester 95/96, Universität Karlsruhe, Fakultät für Informatik, 1996.

[CCT94] CCTA, The Government Centre of Information Systems: IT Infrastructure Library, An Introduction / Configuration Management / Change Management / Quality Management for IT Services, HMSO London, 1994.

[CACA80] Infotech ltd., Computer Audit an Control, Analysis, Infotech State of the Art Report, series 8, number 8; Maidenhead, England 1980.

[CACP80] Infotech ltd., Computer Audit an Control, Invited Papers, Infotech State of the Art Report, series 8, number 8; Maidenhead, England 1980.

[DHM93] James B. Duff, James D. Hunter, David C. Matthews: Process Management - The Vision of Integrated Management, In. Proceedings of the Third International Symposium on Integrated Management, San Francisco, April 1993.

[Dir92] Werner Dirlewanger: Downsizing, Praxis der Informationsverarbeitung und Kommunikation, Heft 15, K.-G. Saur Verlag, Juli 1992.

[Ema94] Michael Emanuel: Open Management - Addressing Real Business Needs, IEEE/IFIP Network Operations and Management Symposium, Orlando, März 1996.

[GMITS] ISO/IEC JTC 1, Information technology - Guidelines for the management of IT-Security (GMITS), ISO/IEC TR 13335.

[GrMa91] I. Gray, S. Manson: The Audit Process, Principles Practise and Cases, Chapman & Hall, 1991.

[Hall96] Jane Hall, Management of telecommunication systems and services: modelling and implementing TMN-based multi-domain management, Springer, 1996.

[Hals96] Fred Halsall: Data communications, computer networks and open systems, 4. Ed., Addison-Wesley, 1996.

[HAW96] Heinz-Gerd Hegering, Sebastian Abeck, René Wies: Corporate Operation Frameworks for Network Service Management, IEEE Communications Magazine Special Issue on Enterprise Networking, April 1996.

[HeAb93] Heinz-Gerd Hegering, Sebastian Abeck: Integriertes Netz- und Systemmanagement, Addison-Wesley, 1993.

[ISO89] ISO 7498-4; Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 4: Management Framework, 1989.

[ISO87] ISO 9001; Quality Systems - Model for Quality Assurance in Design, Development, Production, Installation and Servicing, 1987.

[ISO94] ISO 10164-8; Security Audit Trail Function.

[KöWe97] Dierk König, Frank Wernert: Sicherheitsmanagement-Konzepte für digitale Vermittlungsnetzknoten, Diplomarbeit, Juni 1997.

[Lay96] Wolfgang Ley: Analyse von Log-Informationen, http://www.cert.dfn.de/team/wl/papers/logdaten/, 1996.

[May95] Christian Mayerl: Konzept zur aufwandsbezogenen Abrechnung von verteilten Diensten in einer offenen Systemumgebung, Diplomarbeit, August 1995.

[PGK87] D. A. Patterson, G. Gibson, R. H. Katz: A case for Redundant Arrays of Inexpensive Disks, University California, Berkley CA 1987.

[Sch92] Ingrid Schaumüller-Bichl: Sicherheitsmanagement - Risikobewältigung in informationstechnologischen Systemen, BI-Wissenschaftsverlag, 1992.

[Sch95] Alexander Schill: Cooperative office systems: concepts and enabling technologies, Prentice Hall, 1995.

[SCZ96] Strategisches Computerzentrum Südwest: Qualitätsmanagement-Handbuch, Göppingen, November 1996.

[ScDi94] Heinz Schneeweiss, Jürgen Diercks: Abgestempelt - Qualitätssicherung mit IS0 9000, iX, Heft 4, April 1994.

[Spi82] Gerhard Spilok: Grundfragen der Beweissicherung, Freiburg, Breisgau, Univ., Diss., 1982.

[Tre96] Markus Tresch: Middleware - Schlüsseltechnologie zur Entwicklung verteilter Informationssysteme, Informatik-Spektrum, Heft 19/5, Springer-Verlag, Oktober 1996.

[Wäh93] Gerd W. Wähner: Datensicherheit und Datenschutz: Methoden und Instrumentarien für Computernutzer, VDI-Verl., 1993.

[Wal93] Dieter Wall: Rechner, Netze, Spezialisten - Leistungsangebot der GWDG, Gesellschaft für wissenschaftliche Datenverarbeitung, Göttingen, Oktober 1993.

[Wer94] Markus Wersch: Anwendung, Konzeption und Entwurf eines Werkzeugs zur Koordination komplexer, betrieblicher Arbeitsprozesse, Dissertation, Universität Mannheim, 1994.

[WhPo96] White G., Pooch V.: Cooperating Security Managers: distributed intrusion detection systems, Computers & Security, Vol. 15, No. 5, 1996.

[Wil94] Keith Willets: Service Management - The Drive for Re-engineering, Proceedings of the IEEE Network and Managemet Symposium (Noms´94), Florida, Februar 1994.