DuD
Datenschutz und Datensicherheit

Zentraler Protokollservice

Ein Konzept zur stringenten und datenschutzfreundlichen Verwaltung und Auswertung von Protokolldaten

Sven Thomsen, Martin Rost

Der Umgang mit Protokolldaten war bisher stets das ungeliebte Stiefkind bei der Planung und dem Betrieb von automatisierten Verfahren. Die Autoren stellen ein Konzept zur zentralen Verwaltung und Auswertung von Protokolldaten vor, das auf Standardkomponenten aufbaut. Dabei zeigt sich, dass einige Anforderungen nur durch zusätzliche Sicherheitsmechanismen auf dem Client erfüllt werden können.

Sven Thomsen

Leiter des Referats „Systemdatenschutz“ beim Unabhängigen Landeszentrum für Datenschutz (ULD)

E-Mail: thomsen@datenschutzzentrum.de

Martin Rost

Mitarbeiter im Referat „Systemdatenschutz“ beim Unabhängigen Landeszentrum für Datenschutz (ULD)

E-Mail: rost@datenschutzzentrum.de

Einleitung

Der organisierte, strukturierte Umgang mit Protokolldaten stellt bei zunehmender Komplexität automatisierter Verfahren neue Herausforderungen an IT-Sicherheits- und Datenschutzbeauftragte. Unternehmen und öffentliche Einrichtungen müssen zentrale Protokollservices aufbauen, um den betrieblichen und gesetzlichen Anforderungen zur Protokollierung und dem Umgang mit Protokolldaten gerecht zu werden. Dabei reicht es nicht aus, nur über einen dedizierten zentralen Protokollserver verfügen zu können. Vielmehr muss der gesamte Lebenszyklus von Protokolldaten – vom Erzeugen bis zum Löschen – durch ein einheitliches Verfahren unterstützt werden.

Im Folgenden werden wir zeigen, dass einige Anforderungen nur durch zusätzliche Sicherheitsmechanismen auf dem Client erfüllt werden können.

1 Anforderungen

Die Anforderungen an einen zentralen Protokollservice müssen sicherheitstechnisch konventionell durchdekliniert werden. Der Aufbau eines Protokollservice stellt ein eigenständiges Verfahren zur Verarbeitung – im Allgemeinen personenbezogener – Daten dar. Der Protokollservice muss in einer Client-Server-Architektur aufgebaut werden, um auch für eine große Anzahl von Systemen verwendbar zu sein.

In der folgenden Betrachtung des Protokollservice muss der Begriff „Client“ deshalb im Sinne einer *Protokoll erzeugenden Instanz* verstanden werden. Auf dem Client finden sich eine oder mehrere Protokoll erzeugende Komponenten.

Die Protokoll verarbeitende Instanz wird im Folgenden zur Abgrenzung als *Protokollserver* bezeichnet.

In der folgenden Analyse werden die jeweiligen Anforderungen als Leitlinien formuliert. Als generelle Leitlinie für das Design eines Protokollservice muss gelten:

Protokolleinträge müssen valide sein, datenschutzgerecht gestaltet und verwaltet sowie sicher transferiert und gespeichert werden, um die Verwertbarkeit von Protokolldaten nicht zu beeinträchtigen.

1.1 Verfügbarkeit

Kein Protokolleintrag darf verloren gehen! Die Vollständigkeit eines Protokolls ist eines seiner wichtigsten Gütekriterien. Sowohl die Protokoll erzeugende als auch die Protokoll verarbeitende Instanzen müssen besonderen Verfügbarkeitsanforderungen genügen. Eine erhöhte Verfügbarkeit kann durch das Mehrfachauslegen von kritischen Komponenten hergestellt werden. Ebenso kann durch die Verwendung störungsresistenter Protokolle ein Protokollservice ohne das Doppeln einzelner Komponenten hochverfügbar gestaltet werden.

1.2 Integrität

Kein Protokolleintrag darf nachträglich verändert werden! Alle Protokolldaten müssen frei von Zweifeln über ihre Korrektheit und Authentizität sein. Gerade die Protokoll verarbeitende Instanz muss vorzugsweise durch technische, aber auch durch organisatorische Maßnahmen dafür Sorge tragen, dass die an sie übertragenen Protokolldaten unverändert gespeichert werden.

1.3 Vertraulichkeit

Kein Protokolleintrag darf unberechtigt ausgelesen oder weiterverwendet werden! Durch Sicherheitsmechanismen sowohl bei der Übermittlung zum als auch bei der Ablage der Daten auf dem Protokollserver muss sichergestellt werden, dass nur berechtigte Personen Protokolldaten einsehen und weiterverarbeiten können.

1.4 Zweckbindung

Kein Protokolleintrag mit Personenbezug ohne Zweckbindung! Für Protokolldaten gilt eine strikte Zweckbindung auf die Verwendung für die Datenschutzkontrolle, der Datensicherheit oder des ordnungsgemäßen Betriebes der Datenverarbeitungsanlagen. Ein Protokollservice muss durch technische Maßnahmen eine unberechtigte Auswertung von Protokolldaten für andere Zwecke unterbinden. Es muss festgelegt werden, zu welchen Zwecken Protokolleinträge tatsächlich ausgewertet werden dürfen.

1.5 Isolation

Protokolldaten weg von den Produktionsmaschinen! Das Verfahren „Protokollservice“ muss sauber von anderen Verfahren getrennt und soweit wie möglich isoliert betrieben werden.

Die Systemarchitektur muss eine strikte Trennung zwischen Datenerfassung, Datentransfer, Datenhaltung und –auswertung gewährleisten. Erst durch definierte Übergänge zwischen diesen Phasen kann ein sicherer Protokollservice bereitgestellt werden.

2 Grobkonzept

Um einen in der täglichen Praxis im Rechenzentrumsbetrieb einsetzbaren Protokollservice aufzubauen, sollte er soweit wie möglich auf Standardkomponenten aufgebaut werden. Nahezu jede Organisation, die automatisierte Verfahren in größerem Stil betreibt, hat Know-how zu Datenbanksystemen, Applikationsservern und Betriebssystemen im Haus verfügbar.

Der Protokollservice muss sich auf diese durch langjährigen Einsatz erprobte Standardkomponenten stützen. Ein funktionierendes Sicherheitsmanagement der Hersteller solcher Komponenten bietet üblicherweise ein deutlich höheres Sicherheitsniveau als eine Organisationseinheit für eine Eigenentwicklung bereitstellen kann. Gerade öffentlich im Quelltext verfügbare Software mit Fokus auf ein sicheres Entwicklungsmodell bietet hier eine gute Ausgangsbasis.

Gleichzeitig erleichtert der Einsatz von standardisierten Komponenten die Möglichkeit, den Protokollservice mit Unterstützung externer Dienstleistungsunternehmen aufzubauen, wenn eine starke Trennung vom eigentlichen Verfahrensbetrieb bis herunter auf die Implementierungsebene umgesetzt werden soll.

2.1 Datenerfassung

Verschiedene Komponenten der für ein Fachverfahren benötigten IT-Infrastruktur erzeugen Protokolldaten. Hierbei handelt es sich zum einen um die Protokolleinträge des jeweiligen Betriebssystems, hauptsächlich sind hier Microsoft- oder UNIX-artige Systeme anzutreffen. Aufbauend auf dieser Basis generieren dann unterschiedliche Programme – Datenbanksysteme, Applikationsserver usw. – weitere Logdateien.

Darüber hinaus sind an Fachverfahren in der Regel auch dedizierte Komponenten zur Vernetzung – Router, Switches, Firewalls – beteiligt, die wiederum überwiegend mit eigenen Protokollmechanismen ausgestattet sind.

Um der Vielfalt und unterschiedlichen Ausgestaltung von Protokolldaten Herr zu werden und die Verwaltung des Protokollservers zu vereinfachen, ist für den Client ein Modell mit *lokalen Protokolladaptern und –übersetzern* zu empfehlen. Diese nehmen den Protokolldatenstrom der einzelnen Komponenten entgegen. Der Adapter „spricht“ mit dem Client in dessen „Dialekt“ – als Beispiel UNIX-syslog – aber gegenüber dem Protokollserver eine standardisierte, einheitliche „Sprache“. Die Adapter wandeln die Protokolldaten unter Beibehaltung des Original-Protokolleintrags in ein einheitliches Format, welches den Datentransfer und die spätere Verarbeitung erleichtert.

Diese lokalen Adapter stellen einen sicheren Ausgangspunkt für den Protokollservice dar. Zwischen ihnen und dem zentralen Protokollserver findet eine wechselseitige Authentifizierung statt. So kann ausgeschlossen werden, dass sowohl nicht autorisierte Clients Protokolldaten anliefern, als auch Protokolldaten nur bekannten und autorisierten Servern zur Verfügung gestellt werden.

Die lokalen Adapter sorgen in Verbindung mit dem Protokollserver für ein erhöhtes Maß an Verfügbarkeit, welches mit bekannten Protokollmechanismen nicht erreicht werden kann. Sowohl Client als auch Server versichern sich, dass die jeweilige Gegenstelle noch korrekt arbeitet.

Sollte der zentrale Protokollserver ausfallen, so speichert der lokale Adapter die anfallenden Protokolldaten zwischen, um sie zuzustellen, sobald der Protokollserver wieder erreichbar ist. Sollte ein Client ausfallen, so registriert der Protokollserver diesen Ausfall und generiert seinerseits entsprechende Protokollmeldungen.

Die Adapter sollten bevorzugt als Softwarekomponente auf den Clients installiert werden. Ist dies – zum Beispiel bei Routern oder Switches – nicht möglich, so kann der Adapter auch im Sinne eines *Konzentrators* auf einer Managementstation installiert werden und die Protokolldaten für mehrere Geräte entgegennehmen.

Bei einer Installation auf dem Client kann der Adapter darüber hinaus überprüfen, ob die Protokoll erzeugenden Komponenten korrekt konfiguriert und in Betrieb sind. Ein versehentliches oder absichtliches Deaktivieren beziehungsweise Umkonfigurieren der Protokoll erzeugenden Komponenten wird durch den Adapter erkannt und erzeugt einen eigenständigen Protokolleintrag.

2.2 Datentransfer

Der Adapter auf dem jeweiligen Client übermittelt die Protokolldaten auf einer durch Standard-Verschlüsselungsmethoden – Secure Socket Layer (SSL) und Transport Layer Security (TLS) – abgesicherten Verbindung. Hierbei ist möglichst auf eine Ende-zu-Ende-Sicherheit zwischen Protokoll erzeugender und Protokoll verarbeitender Instanz zu achten, jede Umverschlüsselung oder sonstige Wandlung des Protokolldatenstroms bietet ein zusätzliches Potential für ungewollte Veränderungen.

Das Protokoll zur Übertragung muss denselben Designgrundsätzen folgen, die auch beispielsweise beim Standard-Internet-Protokoll TCP (Transmission Control Protocol) für eine gesicherte Übertragung sorgen. Jedes übermittelte Protokolldatum muss vom zentralen Protokollserver quittiert werden. Sollte eine Quittung ausbleiben, so muss der Adapter auf dem Client

eine nochmalige Übertragung veranlassen (PAR, Positive Acknowledgement with Retransmission).

Der Protokollserver seinerseits darf nur genau dann eine Quittung versenden, wenn er für eine gesicherte Ablage des Protokolldatums gesorgt hat.

2.3 Datenhaltung

Der sicheren und unverfälschten Ablage von Protokolldaten kommt im Protokollservice eine hohe Bedeutung zu. Hier muss auf bereits erprobte Datenbanksysteme zurückgegriffen werden. Nahezu jedes professionelle – sei es kommerziell oder OpenSouce–Datenbanksystem erfüllt die so genannten ACID-Anforderungen:

- Atomizität, **A**tomicity: Eine Transaktion wird entweder komplett ausgeführt oder schlägt fehl. Das Datenbanksystem führt selbst mehrere Anweisungen zur Speicherung eines Protokolldatums so aus, dass am Ende entweder alle Anweisungen oder keine ausgeführt worden sind.
- Konsistenz, **C**onsistency: Eine Transaktion hinterlässt stets einen konsistenten Datenbestand.
- **I**solation: Gleichzeitige stattfindende Transaktionen beeinflussen sich nicht gegenseitig.
- Dauerhaftigkeit, **D**urability: Der Datenbestand bleibt – insbesondere nach beispielsweise Systemabstürzen – konsistent.

Ein klassisches Datenbanksystem bietet somit ein ideales Mittel zur zentralen Datenhaltung von Protokolldaten.

Heutige Datenbanksysteme sind zur performanten Verwaltung auch großer Datenmengen im Terabyte-Bereich konzipiert, so dass auch bei großen Installationen der Protokollservice mit jeder anfallenden Datenmenge fertig wird. Nur eine Organisation der Protokolldaten in *einer* Datenbank kann der Anforderung gerecht werden, dass auf jeden Protokolleintrag zweckorientiert einzeln zugegriffen werden kann.

2.4 Datenauswertung

Für die Datenauswertung können ohne zusätzlichen Aufwand Standard-Reporting-Funktionen des Datenbanksystems oder klassische Reportgeneratoren von Fremdherstellern genutzt werden. Es besteht sogar die Möglichkeit über Programme der üblichen Office-Suiten auf die Datenbasis zuzugreifen.

Problematisch ist jedoch die oft nur mangelhafte Zugriffsteuerung. Gerade durch Kumulationseffekte können hier zusätzliche datenschutzrechtliche Probleme auftreten. Aus diesem Grund sollte auch die Auswertung durch bereits vordefinierte Abfragen und Statistiken streng geregelt werden. Eine „Freistil-Analyse“ mit Data-Mining-Techniken darf nur in Ausnahmefällen freigegeben werden.

Wir empfehlen eine Auswertungsmöglichkeit bereit zu stellen, die schon in Konzeption und Design die Anforderungen einer datenschutzfreundlichen Auswertung von Protokolldaten erfüllt. Eine solche Applikation sollte die Modellierung, den Test, die Freigabe und den kontrollierten Einsatz von Abfragen und Statistiken unterstützen.[1]

Für die Implementierung einer solchen Auswertungsinstanz bieten sich sowohl die in einigen aktuellen Datenbanksystemen integrierten Applikationsserver an. Alternativ sollte auf Standard-Applikationsserver gesetzt werden.

2.5 Datenlöschung

Datenbanksysteme bieten ideale Mechanismen zur strukturierten Datenhaltung und –löschung. Anders als in klassischen, dateisystembasierten Protokolldateien können hier performant Protokolleinträge nach frei definierbaren Parametern gelöscht werden.

Jedoch muss auch die Löschung von Protokolldaten durch technische Maßnahmen abgesichert werden. Die Löschroutinen dürfen genau wie die Algorithmen zur Datenauswertung nicht frei definiert werden, sondern sind im Rahmen der organisationsinternen Abstimmung bereits vor dem Anfallen des ersten Logdatums festzulegen.

3 Fazit

Die grundlegenden Bausteine für einen zentralen Protokollservice sind in den meisten Unternehmen vorhanden. Datenbanksysteme und Applikationsserver gehören zum Standardrepertoire beim Betrieb automatisierter Verfahren.

Leider finden sich sowohl im kommerziellen als auch im OpenSource-Umfeld gerade für die Datenauswertung und -löschung kaum fertige Lösungen, die eine datenschutzfreundliche Analyse von Protokolldaten ermöglichen. Die Realisierung der in diesem Konzept vorgeschlagenen Adapter erzeugt daher einen gewissen Aufwand. Dieser hält sich aber gleichwohl in Grenzen, weil viele benötigte Funktionen in Form von frei verfügbaren Programmbibliotheken bereits vorhanden sind, so dass durch geschickte Wiederverwendung der Aufwand für eine Implementierung kalkulierbar bleibt.

Ein deutlich höherer Aufwand fällt für die Komponenten zur Datenauswertung und –löschung an. Die zum Analysieren und Löschen der Daten genutzten Algorithmen stellen hierbei aber nur ein kleineres Problem dar.

Das Erstellen einer Applikation, die benutzer- und datenschutzfreundlich die Analyse großer Datenmengen ermöglicht, stellt gerade an die Benutzerführung hohe Anforderungen. Doch auch hier existieren bereits gerade aus dem Telekommunikationsbereich Erfahrung mit einer nutzerfreundlichen Aufbereitung komplexer Sachverhalte und großer Datenmengen. Als Beispiel ist auf die zentralen Kontrollzentren der großen Telekommunikationsanbieter zu verweisen.

Wie auch immer, die Notwendigkeit zur stringenten, nachvollziehbaren und sicheren Verarbeitung von Protokolldaten bietet Unternehmen und öffentlichen Einrichtungen genügend Anreize, die erforderlichen Lösungen für eine klassische Vermarktung oder über OpenSource-Ansätze zu realisieren. Nach unserer Einschätzung wird der Markt für Applikationen zur unternehmensweiten, stringenten Verwaltung und Auswertung von Protokolldaten deutlich wachsen. Unternehmen, die sich bereits mit klassischen Infrastruktur-Management-Systemen am Markt positionieren, werden Protokollservices in ihre Produkte integrieren.

[1] Vgl. Beitrag von Rost/Thomsen in diesem Heft.