DuD
Datenschutz und Datensicherheit

Protokollierung bei Identitätsmanagementsystemen

Anforderungen und Lösungsansätze[1]

Martin Meints

Wozu wird Protokollierung bei Identitätsmanagementsystemen eingesetzt? Da Identitätsmanagementsysteme sehr unterschiedliche Aufgaben erfüllen, sind auch die Anforderungen an die Protokollierung unterschiedlich. Dieser Beitrag gibt einen Überblick über unterschiedliche Typen von Identitätsmanagementsystemen, ihre Aufgaben und die daraus folgenden Anforderungen an die Protokollierung. Für nutzerkontrollierte Identitätsmanagementsysteme werden der Stand der Technik und aktuelle Forschungsansätze dargestellt.

Dr. Martin Meints

Mitarbeiter im Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein, vor allem im Projekt „Future of Identity in the Information Society“ (FIDIS)
E-Mail: meints@datenschutzzentrum.de

Einleitung

Der Begriff „Identitätsmanagementsystem“ wird gegenwärtig unterschiedlich verstanden. Bei einer personenzentrierten Sichtweise kann man unterscheiden, wer das Management durchführt und welche technischen Methoden er hierfür einsetzt. So kommt man zu drei Typen von Identitätsmanagementsystemen [MHB05]:

- Typ 1: Zentrale Verwaltung von Benutzerrechten (**A**uthentifizierung, **A**utorisierung, **A**ccounting). Wer verwaltet die Accounts? Organisationen. Wie geschieht dies? Überwiegend unter Einsatz von Verzeichnisdiensten (Directory Services).
- Typ 2: Erstellung von Benutzer- oder Gruppenprofilen (Profiling). Wer verwaltet die Accounts? In der Regel Organisationen. Wie geschieht dies? Überwiegend durch Einsatz von Data Mining (DM) oder Knowledge Discovery in Databases (KDD).
- Typ 3: Nutzerzentrierte, dezentrale Verwaltung von Benutzerrechten. Wer verwaltet die Accounts? Der Nutzer selbst. Wie geschieht dies? Überwiegend durch Einsatz von derzeit noch wenig verknüpften Hilfsprogrammen wie Passwortmanagern, Formfillern oder Anonymisierungsdiensten.

So unterschiedlich die Methoden des Identitätsmanagements sind, so unterschiedlich sind auch die Ziele, Anforderungen und technischen Ansätze zur Protokollierung. Diese sollen in diesem Artikel behandelt werden.

1 Typ 1 IMS Zentrale Verwaltung

Typ 1 Identitätsmanagementsysteme haben sich in den letzten Jahren von dezentralen, oft applikationsspezifischen Benutzerverwaltungen zu einer zentralen Infrastruktur in Organisationen entwickelt. Mit Meta-Directories und Federated Identity Management stehen darüber hinaus auch technische Instrumente zur Verfügung, Verzeichnisdienste über die Grenzen von so genannten Forrests oder Realms und damit unter Umständen auch über Organisationsgrenzen hinaus miteinander zu verbinden. Identitätsmanagement ist damit zu einer organisatorischen Kernanwendung geworden, die oftmals sicherheitskritisch ist. Unter räumlichen und Zuständigkeitsgesichtspunkten können Federated Identitymanagements eine dezentrale Infrastruktur mit hohen Anforderungen an die multilaterale Sicherheit darstellen.

1.1 Anforderungen an die Protokollierung

> Die inhaltlichen Anforderungen an die Protokollierung innerhalb von Typ 1 Identitätsmanagementsystemen werden in der Regel von den Sicherheitsanforderungen der Daten bestimmt, für die diese Systeme Zugang und Zugriff verwalten.

In Fällen, in denen diese Daten geringen Sicherheitsanforderungen unterliegen oder öffentlich sind, reicht es oftmals, gescheiterte Authentifizierungen, Kontosperrungen oder technische Fehler zu protokollieren. Dies entspricht auch dem Grundsatz der Datensparsamkeit.

Sind die Sicherheitsanforderungen höher, werden häufig auch weitere Daten wie

[1] Teile dieser Arbeit wurden von der Europäischen Union mit Mitteln des Projektes „Future of Identity in the Information Society“ (FIDIS) gefördert.

z.B. erfolgreiche Authentifizierungen und Zugriffe auf einzelne Dateien mit Datum und Uhrzeit gespeichert, um jeglichen Zugriff auf die sensiblen Daten zu dokumentieren und gegebenenfalls nachvollziehbar zu machen.

Derartige Protokolldaten sind personenbezogene Daten im Sinne des Bundesdatenschutzgesetzes (BDSG). Sie sind mit dem Verwendungszweck im Verfahrensverzeichnis für das Identitätsmanagement zu behandeln und unterliegen im operativen Betrieb typischerweise hohen Sicherheitsanforderungen zur Gewährleistung von Vertraulichkeit und Integrität.

Technisch bieten die meisten Verzeichnisdienste Systemadministratoren den uneingeschränkten Vollzugriff auf alle Protokolldaten. Dieser lässt sich oftmals auch nicht einschränken. In diesem Falle sind organisatorische Regelungen notwendig. Diese sollten z.B. enthalten:

- Verbot des unautorisierten Zugriffs auf Protokolldaten (Nutzungsverbot mit Erlaubnisvorbehalt),
- Umsetzung des 4-Augen-Prinzips beim Zugriff,
- Dokumentation vorgenommener Zugriffe mit Grund und Genehmigenden,
- Dokumentation vorgenommener Änderungen (z.B. Löschungen) mit Grund und Genehmigendem,
- Regelungen für Löschfristen von Protokolldaten oder
- Regelungen zu internen Audits über die Umsetzung der o.g. Regelungen.

Technisch lässt sich die Umsetzung solcher Regelungen durch dedizierte Protokollserver unterstützen, wie sie z.B. im Bereich von Firewalls und Intrusion Detection / Intrusion Prevention Systemen eingesetzt werden.

2 Typ 2 IMS: Profiling

Typ 2 Identitätsmanagement, auch Profiling [HB05] genannt, weist eine große Anwendungsbreite auf. Es wird etwa für Marketingzwecke eingesetzt, um Kunden zu clustern oder ihr vermutliches Kaufverhalten vorauszusehen und zu beeinflussen. Ein weiterer großer Anwendungsbereich ist das so genannte Scoring, bei dem die finanzielle Potenz von Kunden bzw. das Risiko eines finanziellen Ausfalls etwa bei Krediten betrachtet wird.

2.1 Funktionen

Beim Profiling kann man grundsätzlich drei Funktionsträger beobachten, die personell oftmals nicht zusammenfallen:

- Datensubjekt (Person, über die das Profil erstellt wird),
- Datencontroller (Operator),
- Datennutzer (Person oder Organisation).

Darüber hinaus kann man beim Profiling grundsätzlich zwei Modi unterscheiden:

- Eine Optimierungsphase, in der Algorithmen ausgewählt und deren Parameter optimiert werden und
- Eine Anwendungsphase, in der Basisdaten zu Profilen verdichtet werden.

Bei Einsatz von bestimmten, evolutionären Algorithmen (z.B. Heuristik, Neuronale Netze) verändern sich die Algorithmen dauernd und selbstständig in Abhängigkeit von den verarbeiteten Daten und Zielvorgaben des Datencontrollers.

2.2 Anforderungen an die Protokollierung

Grundsätzlich sind beim Profiling für die Protokollierung die Bestimmungen des BDSG anzuwenden.

> Darüber hinaus sehen aktuelle Standards für das Data Mining, wie etwa der Cross Industry Standard Process for Data Mining (CRISP-DM)[2] für die Optimierungsphase eine umfangreiche Dokumentation und Protokollierung der eingesetzten Ausgangsdaten, der Parameterberechnungs- und -optimierungsläufe, der Ergebnisse und der Qualitätssicherung vor. Die Dokumentation soll typischerweise in einem Report erfolgen.

In einigen Fällen kann die Optimierungsphase unter Einsatz des so genannten Privacy Preserving Data Mining erfolgen. Hierbei werden z.B. die Daten anonymisiert. Wird dies so durchgeführt, dass eine Deanonymisierung nicht möglich ist, findet das BDSG keine Anwendung. Eine Übersicht über aktuelle Ansätze zum Privacy Preserving Data Mining ist an der University of Alberta in Kanada erstellt worden.[3]

In der Anwendungsphase bestimmen Sicherheitsanforderungen, die sich teilweise aus dem Datenschutz herleiten, Art und Umfang der Protokollierung. Die Protokollierung sollte so gestaltet sein, dass sie die Erfüllung der folgenden Anforderungen aus dem BDSG ermöglicht:

- Transparenz und Auskunftsanspruch; dem Datensubjekt sind jederzeit auch rückwirkend Ausgangsattribute, Ablauf und Ergebnis des Profiling zu erläutern.
- Jederzeit ist eine Korrektur fehlerhafter Basisdaten möglich.

Teilweise werden die genannten Anforderungen an die Protokollierung unterlaufen. Durch die Schufa beispielsweise werden Ausgangsdaten und Scoring-Werte nicht dauerhaft gespeichert bzw. sofort nach der Übermittlung an den Datennutzer (in der Regel ein Unternehmen der Finanzwirtschaft) wieder gelöscht (ULD06).

Auskunfts- und Berichtigungsgesuche des Datensubjekts über in der Vergangenheit berechnete Scoring-Werte laufen in diesem Fall ins Leere, was eine Verletzung der einschlägigen Vorschriften des BDSG darstellt. Technisch könnte eine Lösung mittels geeigneter Protokollierung erzielt werden. Die Schufa plant bis Ende 2006 eine Änderung der beschriebenen Praxis (ibid.).

Die Anforderungen an die technische und organisatorische Sicherheit der Protokolldaten entsprechen denjenigen der Typ 1 Identitätsmanagementsysteme.

3 Typ 3 IMS: Nutzerkontrolle

> Hansen et al. [IPTS03: 89] haben bereits 2003 das „History-Management“ als eine wesentliche Funktion des nutzerkontrollierten Identitätsmanagements dargestellt. Das Ziel des History-Managements ist die Kontrolle des Nutzers über die Daten, die er im Zuge einer durch Identitätsmanagement gestützten Kommunikation weitergegeben hat. Dabei werden eigene Log-Dateien als eine wesentliche Informationsquelle angeführt.

3.1 Protokollierung

Was kann typischerweise Inhalt der Protokollierung sein? Neben rein technisch auf dem System des Nutzers erfassbaren Transaktionsdaten (Wer? Wann? Welche Informationen? An wen, welches Zielsystem?) können weitere Daten für eine umfassende History der Transaktionen mit Organisationen (öffentliche Verwaltung, Unternehmen) nötig sein:

[2] Siehe http://www.crisp-dm.org
[3] Siehe http://www.cs.ualberta.ca/%7Eoliveira/psdm/pub_by_year.html

- Authentifizierungsinformationen des Diensteanbieters, z.B. Zertifikate,
- Datenschutzrelevante Teile der AGB des Empfängers (z.B. in Form einer Datenschutzerklärung oder policy),
- Persönliche Anmerkungen und Kommentare zur jeweiligen Transaktion.

Auch wenn sie sich bislang bei Anbietern von Diensten und in Anwendungen für Nutzer noch nicht breit durchgesetzt haben, so bietet P3P[4] (Platform for Privacy Preferences) ein Protokoll, dass die strukturierte und standardisierte Übermittlung einer Datenschutzerklärung erlaubt. Dies ist eine Grundlage für eine automatisierte Auswertung innerhalb eines History-Managements.

Aus Datenschutzsicht ist das Protokollieren eigener Log-Daten für den persönlichen Gebrauch unkritisch, auch wenn personenbezogene Daten von Kommunikationspartnern gespeichert werden. Dies ändert sich jedoch, wenn das Log im professionellen Kontext, etwa von Freiberuflern, verwendet wird. Dadurch wird der Nutzer selber zur Daten verarbeitenden Stelle, die die einschlägigen Datenschutzbestimmungen anwenden muss.

Unter dem Gesichtspunkt der IT-Sicherheit sind einige Anforderungen zu beachten. Typischerweise sind die Anforderungen bei privater Nutzung an die Verfügbarkeit nicht sehr hoch. Die Datensicherung gewinnt aber an Bedeutung, da die Qualität des History-Managements vom Zeitraum abhängt, über den Log-Daten zur Auswertung zur Verfügung stehen. Außerdem erstellt der Nutzer eine Datensammlung über sich selbst, die auch für andere, nicht autorisierte Nutzer interessant sein kann. Die Vertraulichkeit der Log-Daten und die Sicherheit der Systeme, auf denen diese verarbeitet werden, gewinnt damit erheblich an Bedeutung.

Je nach Ziel des History-Managements kann auch die Integrität einschließlich der Aspekte Authentizität und Nichtabstreitbarkeit eine steigende Bedeutung erlangen. Dies wird in den folgenden Betrachtungen der existierenden Ansätze und der aktuellen Forschung noch näher beleuchtet. Insgesamt erfordert ein umfassendes History-Management ähnlich wie eGovernment oder eBusiness vom Nutzer eine Professionalisierung des IT-Systemmanagements.

[4] Siehe http://www.w3.org/P3P/#what

3.2 Stand der Technik

Die Praxis ist noch nicht so weit, als dass nutzerseitige Protokollierung und Auswertung alltäglich wären. Bislang bieten Standardanwendungen nur rudimentäre Funktionen. Beispiele hierfür sind die History im klassischen Browser oder das Mailarchiv in E-Mailclients. Diese Grundfunktionen lassen in der Regel keine automatische Auswertung hinsichtlich der übermittelten personenbezogenen Daten zu.

Wesentlich weiter entwickelt sind Ansätze von Brückner wie das Data Journal [Brü03] oder dessen Weiterentwicklung, das IJournal[5]. Hierbei handelt es sich um einen lokalen http-Proxy, der den Datenverkehr eines Mozilla-Browsers mitloggt und später eine gezielte Auswertung unter Datenschutzgesichtspunkten durch den Nutzer erlaubt. Diese Entwicklung wird derzeit im Rahmen des MozPETs-Projektes[6] fortgesetzt [Brü05]. Diese Ansätze sind jedoch auf Daten beschränkt, die über den Dienst WWW übermittelt werden.

In speziellen Fällen, in denen es auf die Gerichtsverwertbarkeit elektronischer Dokumente ankommt, kann ein elektronischer Zeuge (e-Witness) oder elektronischer Notar (e-Notary) eingesetzt werden [IPTS03: 70-72]. Hierbei wird die Gerichtsverwertbarkeit von übermittelten Daten und Unterlagen (einschließlich Verträgen) über eine PKI und elektronische Signaturen (Sicherstellung von Vertraulichkeit und Integrität) sowie einer externen Hinterlegung bei einem Zeugen (e-Witness[7]) oder Notar (e-Notary[8]) erreicht. Gegenwärtig wird auch an XML-Standards für die Übermittlung der Daten gearbeitet (LegalXML).[9] Eine Auswertung von übermittelten Daten unter dem Gesichtspunkt des Datenschutzes ist nicht Kern dieser Konzepte.

3.3 Forschung zum History-Management

Seit 2004 wird im Rahmen des Projektes PRIME (Privacy and Identity Management for Europe) an einem integrierten Prototyp für Typ 3 IMS gearbeitet. Dieser soll auch die Funktion „Data Track“ beinhalten, die gestützt auf eine Datenbank die Darstellung der übermittelten personenbezogenen Daten und der Empfänger erlaubt [FHAH05]. Zudem soll „Data Track“ dem Nutzer Vorschläge und Handlungsoptionen unterbreiten, wenn die übermittelten Daten oder deren Empfänger nicht den Erwartungen des Nutzers entsprechen (z.B. bei Phishing).

Auch eine Simulation, die den Nutzer mit verschiedenen Datenübermittlungsvarianten testen lässt, welche personenbezogenen Daten an wen übermittelt werden, ist in PRIME diskutiert worden [Pet05]. Eine solche Simulation ist ohne Informationen zur Datenschutz-Policy und den zugrunde liegenden Workflows durch die Daten verarbeitenden Stelle nicht denkbar.

Hinsichtlich der erreichten IT-Sicherheit sind alle diese beschriebenen Ansätze entscheidend von der Sicherheit der Systeme abhängig, auf denen sie ausgeführt werden. Diese Formen des History-Managements sind für den Nutzer sehr hilfreich, in juristischen Streitfällen aber nur ein der „freien Würdigung“ des Gerichts unterliegender Beweis von vielen. Die Protokolle und die daraus gewonnenen Erkenntnisse sind also nur mit Einschränkungen geeignet, um Rechtsansprüche aus Transaktionen unmittelbar durchsetzen zu können.

In dieser Hinsicht weiterentwickelt ist der Konzeptansatz der „anhaftenden Policies“ (Sticky Policies), der 2002 von Karjoth und Hunter [KaHu02] vorgestellt und von Casassa Mont et al. [CMPB03] weiterentwickelt worden ist. Kernidee dieses Konzeptes ist es, personenbezogene Daten stets mit einer ausgehandelten Datenschutz-Policy zu versehen und diese auch bei Datenübermittlung an Dritte den Daten weiter anhaften zu lassen.

Bei der Aushandlung und Übermittlung werden Daten und Policy darüber hinaus ähnlich wie beim e-Witness durch eine vertrauenswürdige dritte Partei gespeichert. Im Unterschied zum e-Witness wird hier aber die Vertraulichkeit und Integrität der übermittelten Daten nicht durch elektronische Signaturen auf der Basis einer PKI sichergestellt, sondern unter Einsatz eines Trusted Platform Modules (TPM ab Version 1.1) und eines vertrauenswürdigen Betriebssystems (Trusted OS). Dieser Ansatz wird auch im Projekt PRIME weiterverfolgt [FHAH05].

[5] Siehe http://www.ito.tu-darmstadt.de/projects/prima/index_de_html

[6] Siehe http://mozpets.sourceforge.net/

[7] Siehe z.B.: http://www.entrust.com/news/files/01_23_01_676.htm

[8] Siehe t.B.: http://www.cordys.com/de/Products/Cordys_enotary_overview.htm

[9] Siehe http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=legalxml-enotary

4 Fazit

Die Anforderungen an die Protokollierung bei unterschiedlichen Typen von Identitätsmanagementsystemen unterscheiden sich stark in Abhängigkeit von der jeweiligen Funktion. Dient die Protokollierung in dem Typ 1-Identätsmanagement vor allem der Datensicherheit, so steht bei dem Typ-2-Identitätsmanagement daneben auch die Qualität im Mittelpunkt. Dabei sollte die Protokollierung dem Datensubjekt Transparenz, Auskunft und Berichtung fehlerhafter Daten auch rückwirkend ermöglichen.

Bei dem Typ-3-Identitätsmanagement steht dagegen die Übersicht des Nutzers über die Daten, die er selber im Zuge unterschiedlicher Kommunikation übermittelt hat, im Mittelpunkt (History-Management). Die aktuelle Forschung setzt sich damit auseinander, wie dies effektiver, sicherer und gerichtsverwertbarer als bisher geschehen kann.

Literatur

MHB05 Meints, M., Hansen, M. Bauer, M. (Hrsg.), *FIDIS Deliverable D3.1 – Overview on Identity Management Systems*, Franfurt a.M. 2005. Download siehe http://www.fidis.net/487.0.html

HB05 Hildebrandt, M., Backhouse, J. (Hrsg.), *FIDIS Deliverable D7.2 – Descriptive Analysis and Inventory of Profiling Practice*, Frankfurt a. M. 2005. Download siehe http://www.fidis.net/487.0.html

IPTS03 Institute for Prospective Technological Studies (IPTS), *Identity Management Systems: Identification and Comparison Study*, Sevillia 2005. Download siehe http://www.datenschutzzentrum.de/projekte/idmanage/study.htm

ULD06 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), *Scoringsysteme zur Beurteilung der Kreditwürdigkeit – Chancen und Risiken für Verbraucher*, Berlin 2006, S. 34. Download siehe http://www.bmelv.de/cln_045/nn_752314/SharedDocs/downloads/02-Verbraucherschutz/Finanzdienstleistungen/scoring,templateId=raw,property=publicationFile.pdf/scoring.pdf

Brü03 Brückner, L. *Aktiver Datenschutz mit Data Journals*, DuD 5/2003.

Brü05 Brückner, L., Voss, M., 'MozPETs – a privacy enhanced Web Browser', *Proceedings of the Third Annual Conference on Privacy, Security and Trust (PST05)*. St. Andrews, New Brunswick, Canada; October 12-14, 2005. Download siehe http://www.ito.tu-darmstadt.de/projects/prima/index_de_html

FHAH05 Fischer-Hübner, S., Andersson, C., Holleboom, T., *PRIME Deliverable D14.1.a, Framework Document V1*, St.-Stevens-Woluwe 2005. Download siehe http://www.prime-project.eu.org/public/prime_products/deliverables/fmwk/

Pet05 Pettersson, J. S., *PRIME Deliverable D06.1.c HCI guidance and proposal*, St.-Stevens-Woluwe 2005. Download siehe http://www.prime-project.eu.org/ public/prime_products/deliverables/arch/

KaHu02 Karjoth, G., Hunter, M., 'A Privacy Model for Enterprises', IBM Research, Zürich, *15th IEEE Computer Foundations Workshop*, Keltic Lodge, Canada 2002.

CMPB03 Casassa Mont, M., Pearson, S., Bramhall, P., *Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforcable Tracing Services*, HP Laboratories Bristol, Bristol 2003. Download siehe http://www.hpl.hp.com/techreports/2003/HPL-2003-49.pdf