DuD
Datenschutz und Datensicherheit

Die Datenschutzkonsole

Ein neuer Versuch über eine alte Idee

Martin Rost, Sven Thomsen

Wie gelangt man datensparsam, zweckgerichtet und sicher zu relevanten, möglicherweise sogar standardisierten Protokollmeldungen? Und wie lassen sich diese Protokollmeldungen kontrollieren bzw. beobachten und effektiv auswerten? Die Lösung könnte in einer gesonderten Datenschutzkonsole liegen, deren Grundzüge von den Autoren beschrieben werden.

Martin Rost

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

E-Mail: rost@datenschutzzentrum.de

Sven Thomsen

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

E-Mail: thomsen@datenschutzzentrum.de

Einleitung

Mit den wachsenden Anforderungen an die Leistungsfähigkeit der IT-Systeme in Wirtschaft, Verwaltung und Gesellschaft gewinnt die Protokollierung der wesentlichen Systemfunktionen an Bedeutung. Die Protokollierung dient zum Nachweis, dass das IT-System, aber auch Administratoren und Nutzer die formulierten Vorgaben der Security und Privacy Policy einhalten. Ohne eine revisionssichere Protokollierung können technische Fehler, Bedienungsfehler, Missbräuche und sonstige Verstöße gegen die Vorgaben nicht erkannt und behoben werden.

Angesichts der Bedeutung der Protokollierung wäre zu erwarten, dass die Hersteller der IT-Systeme von den Betriebssystemen bis zu den Anwendungen für eine aussagekräftige und revisionssichere Protokollierung längst gesorgt hätten, indem sie die relevanten Meldungen in einem standardisierten Format bereitstellen. Weil und solange dies nicht der Fall ist, könnte Abhilfe durch eine gesonderte Datenschutzkonsole geschaffen werden. Sie hätte gleichzeitig den Vorteil, als Netzknoten der Protokollierung von Betriebssystem und Anwendungen die Kontrolle des gesamten IT-Systems zu unterstützen. Das hier vorgestellte Konzept folgt unseren Überlegungen zur Trennung von Protokoll-Agenten und Protokollserver.[1]

1 Anforderungen

Wir nähern uns den Anforderungen an die Datenschutzkonsole zunächst über die Frage, welche Funktion die Protokollierung erfüllen soll, um den Umfang der Protokollierungen zu umreißen.

1.1 Funktion der Protokollierung

„Ein Protokoll hält oder legt fest, zu welchem Zeitpunkt (absolut) oder in welcher Reihenfolge (relativ) welche Entität (wer oder was) welche Operation gerade ausführt, ausgeführt hat oder ausführen wird. Protokollierung bezeichnet dabei die Operation des Festlegens bzw. Niederschreibens der drei Protokollbestandteile Zeitpunkt, Entität, Operation.“[2]

Die Funktion des Protokollierens besteht also darin, *„adressierbare Entitäten anhand ihrer Operationen zu beobachten oder beobachtbar zu machen, um Irritationen bzw. Fehler im Nachhinein analysieren oder gegenwärtig oder zukünftig vermeiden zu können.“*

> Eine Datenschutzkonsole muss also gewährleisten, dass sie auf der *Produktionsseite* die drei Funktionen Zeitstempel, Entität und Operation datenschutzgerecht festlegt und auf der *Auswertungsseite* die Protokolldaten zu kontrollieren gestattet.

1.2 Umfang der Protokollierung

Die Datenschutzkonsole eines modernen IT-Systems muss demnach mindestens folgende Protokolle erfassen:

- Technische Logdaten über die Installation, Konfiguration und den Betrieb des *Betriebssystems*,
- Technische Logdaten über die *Netzwerk*funktionalitäten (Server, Router, Firewall etc.),
- Technische Logdaten über die Funktionen der *Applikation*(en),
- Protokolldaten über die *Authentisierung* und *Autorisierung* der Nutzer,
- Protokoll-Metadaten für Eigenschaften von *Dokumenten und*
- Protokoll-*Workflow*-Daten.

[1] Vgl. Thomsen/ Rost, Zentraler Protokollservice (in diesem Heft).

[2] Wikipedia (Stand: 2006.04.03).

1.3 Aufgabe der Datenschutzkonsole

Damit Datenschutz möglich ist, muss ein System transparent gestaltet sein. Soweit mit dem System personenbezogene Daten verarbeitet werden, bedarf es eines Sicherheitskonzeptes, mit dessen Hilfe organisatorische Regelungen und technische Maßnahmen geplant und implementiert werden.

Die ordnungsgemäße Funktion des Systems sowie die Einhaltung und Wirksamkeit der technischen Maßnahmen wird durch die Protokollierung der System- und Sicherheitsfunktionen dokumentiert. Hierbei müssen verschiedene Tätigkeiten unterschieden werden. Administratoren können sowohl Routineaufgaben im Rahmen des Operating wie Wartung und Pflege eines Systems durchführen als auch durch administrative Eingriffe das System verändern. Nutzer verwenden die Funktionen des jeweiligen Systems um beispielsweise Daten einzusehen oder zu ändern.

Ob diese Maßnahmen auch wirklich ordnungsgemäß funktionieren, wird durch die Protokollierung der System- und Sicherheitsfunktionen gewährleistet. Hierbei wird typischerweise zwischen der Tätigkeit der Administratoren und der der Nutzer unterschieden. Die Aufgabe der Datenschutzkonsole besteht also darin, das Datenschutz- und Sicherheitsmanagement für Zwecke der Datenschutzkontrolle zu ermöglichen, indem es den IST-Zustand erfasst und einen Vergleich mit dem SOLL-Zustand ermöglicht.

Die Datenschutzkonsole ist also Werkzeug für den Datenschutz, sie muss aber auch selbst Datenschutzanforderungen erfüllen. So muss sie datensparsam gestaltet sein (§ 3 a BDSG, § 4 Abs. 1 LDSG SH) und die von ihr verarbeiteten Daten unterliegen einer besonderer Zweckbindung (§ 31 BDSG, § 13 Abs. 6 LDSG SH).

2 Produktion

Die Kernidee für die Gestaltung der Produktionsseite besteht darin, dass die Datenschutzkonsole nicht die Protokollierungsdaten der Applikationen konfiguriert, sondern den *Protokolldaemo*n, über den exklusiv sämtliche Protokollkommunikationen abgewickelt werden.

> Die Datenschutzkonsole dient unter diesem Blickwinkel dazu, dass die bislang nicht standardisierten und semantisch oftmals beliebigen Protokollierungsmeldungen der Betriebssysteme und Applikationen empirisch untersucht werden.

2.1 Grundfunktion

Nach der Untersuchung und der Festlegung, welche der Meldungen zu welchen Zwecken protokolliert werden sollen, lässt sich mit Hilfe der Datenschutzkonsole ein *Mapping* für den Protokollagenten bzw. Protokolldaemon erzeugen. Auf diese Weise werden aus den Meldungen der Applikationen an den Daemon weitgehend standardisierte Meldungen, die in der Folge eine automatisierte Auswertung stark erleichtern.

Für das Mapping ließe sich an die Verwendung einer XML-Syntax denken. Sie muss die Meldung der Applikation aufnehmen und zusammen mit einer standardisierten und aussagekräftigen Meldung an den Protokolldaemon weiterreichen, so dass auch die Form der zugelassenen Auswertungen festgehalten wird. Darüber hinaus müssen die Protokollierungsparameter verschiedener Applikationen über die Konsole gut dokumentiert gesetzt werden können.

Die Protokolleinträge müssen also so konfiguriert werden, dass sie die rechtlichen und betrieblichen Anforderungen des Datenschutzes und der Datensicherheit, insbesondere die der Kontrolle und der Revision erfüllen.

2.2 Qualitätsdaten

Voraussetzung einer aussagekräftigen Protokollierung ist, dass die Applikationen qualitativ hochwertigere Protokolldaten erzeugen. Worin bestehen Qualitätsprotokolldaten?

Für das Mapping der Protokolldaten ist mindestens auf die folgenden Eigenschaften der Protokolleinträge zu achten:

- *Relevanz:* Hat die Protokollmeldung einen tatsächlich verwertbaren Informationsgehalt über den Zustand des IT-Systems?
- *Validität*: Entsprechen die (Vertextungen der) Protokollmeldungen des Betriebssystems oder der Applikation den Tatsachen?
- *Reliabilität*: Sind die Meldungen bei gleichen oder nahe verwandten Vorfällen ähnlich, stabil und reproduzierbar?
- *Verständlichkeit*: Ist der Protokolleintrag für eine Auswertung und Reaktion hilfreich? Hierbei stellt sich die Frage, an welcher Stelle die Protokollmeldungen textlich ausformuliert sein sollten oder ob formalisierte (codierte), aber unverständliche Maschinenmeldungen möglicherweise allein aus Performancegründen angemessener sind. Bei einer Entscheidung für eine codierte Form der Meldungen sollte die Vertextung spätestens vor der Kontrolle der Protokolle einsetzen.
- Trägt die Auswahl der Protokolldaten den Analysezwecken einerseits, aber auch den Interessen der Betroffenen *datensparsam* und *zweckkonform* Rechnung? Hierzu gehört bspw., dass für eine Auswertung nicht aussagekräftige Daten standardmäßig gelöscht werden.

2.3 Konfiguration

Die Leistungsfähigkeit der Datenschutzkonsole ist von ihrer Konfiguration abhängig. Es muss vor ihrem Betrieb geklärt sein, zu welchem Zweck welche Protokolleinträge erforderlich sein werden. Diese Festlegung erfordert die Mitwirkung des betrieblichen bzw. behördlichen Datenschutzbeauftragten, weil die Protokolldaten ihn bei der Erfüllung seiner Überwachungsaufgabe unterstützen.

Da die Protokolldaten regelmäßig auch Auskunft über das Verhalten und die Tätigkeit zumindest der Administratoren, häufig aber auch der beschäftigten Nutzer geben können, wird die Festlegung der Protokollierung und ihrer Verwendung auch der Mitbestimmung durch den Betriebsrat bzw. Personalrat bedürfen.

Für die Konfiguration der Datenschutzkonsole selbst bzw. der Änderungen ihrer Einstellungen bedarf es zusätzlicher Sicherheitsmaßnahmen, zu denen die Einhaltung des Vier-Augen-Prinzips im Fall solcher Einstellungen, die Protokollierung der Konfiguration sowie ihre Kontrolle gehört.

3 Auswertung

Die Datenschutzkonsole soll helfen, die Qualität der drei in der Definition aufgeführten Bestandteile eines Protokolls jeweils in einem Überblick darzustellen. Die Datenschutzkonsole muss also Aussagen ermöglichen wer, wann, was in dem IT-System getan hat:

3.1 Funktionen

- Das *Zeitstempelformat* in den Protokolleinträgen ist in ein menschlesbares Format zu übersetzen. Aus dem Zeitstempel muss sich ergeben, ob die lokale Server-Zeit, die LAN-Zeit oder eine Zeit von einem externen Zeit-Server erhoben und gespeichert wird.
- Zwischen verschiedenen Protokolldatenbeständen muss ein *Abgleich* erlaubt sein. Ein typischer Fall besteht darin, die Einträge aus dem Authentisierungsprotokoll mit den Logeinträgen der Tätigkeit der Systemadministration zu vergleichen.
- Auch sollte der Vergleich von Protokolldaten *über Organisationsgrenzen* hinweg unterstützt werden, um das Zusammenspiel verschiedener, aber aufeinander bezogener Operationen verschiedener IT-Systeme in Beziehung setzen zu können.
- Von Bedeutung ist für eine Auswertung, inwieweit verschiedene Protokolleinträge zueinander passen, die die gleiche Transaktion an verschiedenen Orten betreffen. In dieser Problemstellung kann es sinnvoll sein, die *Protokollierung einer Transaktion* bzw. Kommunikation von einer dritten, unabhängigen Instanz, etwa in Form eines E-Notary (vgl. [1]), vornehmen zu lassen. Ohne eine dritte Instanz wären dann möglicherweise nur diejenigen Einträge als gültig zu akzeptieren, die sich auf beiden Seiten plausibel aufeinander beziehen.
- Eine der Hauptfunktionen der Datenschutzkonsole wird darin bestehen, *unterschiedliche Views* auf den Protokolldatenbestand zu formulieren. Wenn sich ein Systemadministrator allein für technische Systemdetails interessiert, sollten personenbeziehbare Daten gar nicht erst erscheinen. Ein Datenschutzbeauftragter muss jedoch, um seine Kontrollfunktion erfüllen zu können, sämtliche Tätigkeiten der Administratoren überprüfen können.
- Die Datenschutzkonsole könnte schließlich *pseudonymisierte Logfiles* verwalten bzw. sie mit Unterstützung eines entsprechenden Dienstes zu definierten Zwecken und nach einer entsprechenden Freigabe auflösen.
- Die Datenschutzkonsole ermöglicht eine Kontrolle der Protokolle nicht nur zeitgleich, sondern über die Funktion ihrer *Dokumentation* auch nachlaufend. Diese Aufgabe ist insbesondere zum Schutz der Administratoren selbst sinnvoll und erforderlich. Sie hat aber auch Bedeutung zur Kontrolle einer Auftragsdatenverarbeitung, damit ein Auftraggeber die Erfüllung seiner Weisungen durch den Auftragnehmer anhand der automatisierten Protokolle kontrollieren kann.
- Die Datenschutzkonsole ermöglicht eine differenzierte und automatisierte *Löschung von personenbezogenen Protokolldaten* je nach Verwendungszweck und in Abhängigkeit von aktuellen Vorfällen. Auf diese Weise unterstützt die Datenschutzkonsole eine datensparsame Speicherung der Protokolldaten.

3.2 Datenschutzmonitor

Ein praktisches Problem in der Analyse von Protokolldaten ergibt sich aus der Zeitdifferenz zwischen dem protokollierten Ereignis und seiner Auswertung. Im Ergebnis ist eine gezielte Reaktion auf ein relevantes Ereignis immer erst mit einem je nach Vorfall und den zu seiner Beseitigung verfügbaren Ressourcen erheblichen Zeitverzug möglich.

Um diesem Problem abzuhelfen, sollte die Datenschutzkonsole um einen Datenschutzmonitor erweitert werden. Dieser Monitor müsste in Anlehnung zu den Infrastruktur-Management-Systemen in den Rechenzentren funktionieren, die die Zustände der verschiedenen Systeme auf wenigen Bildschirmen zusammengefasst und übersichtlich darstellen.

Entsprechend muss die Datenschutzkonsole durch deutliche akustische oder optische Warnsignale datenschutzkritische Zustände signalisieren, um sofortige Gegenmaßnahmen zu ermöglichen. Dies sollte bspw. der Fall sein, wenn an zentralen Einstellung des IT-Systems Veränderungen oder Änderungen an einem Verzeichnis ohne eine ausreichende Berechtigung versucht werden. Auch statistisch signifikante Protokolleinträge, die von einem definierten Normalzustand abweichen, könnten signalisiert werden.

Schließlich könnten die Warnmeldungen auch unterschiedlich adressiert werden. So könnte bei Eingriffen durch die Administration standardmäßig eine Meldung an den Datenschutzbeauftragten der Organisation erfolgen.

3.2 Sicherheit prüfen

Die Datenschutzkonsole sollte ferner den Sicherheits- und Datenschutzzustand von Systemen untersuchen und dokumentieren, also im weiteren Sinne protokollieren. Diese Protokollierung könnte bspw. die Inventarisierung von Hard- und Software erfassen, Abhängigkeiten zwischen Applikationen festhalten und Zugriffsrechte auf ihre Plausibilität prüfen sowie entsprechende Reports auswerfen.

Die Datenschutzkonsole müsste außerdem gestatten, die Sicherheitsaspekte im Zusammenspiel zwischen den Applikationen, dem Protokolldaemon und dem Speicherort der Protokolldaten zu gestalten und ihre Überprüfung zu ermöglichen. Auf dieser Weise sollte sichergestellt werden, dass Anwendungen sich gegenseitig authentifizieren und Protokolldaten einer Applikation nicht auf dem Weg zum Protokolldaemon oder vom Daemon zum Protokollserver manipuliert werden können.

Die Datenschutzkonsole soll auch die Aufdeckung unterstützen, wenn ein Protokollservice kompromittiert worden ist.[3]

4 Fazit

In der Datenschutzkonsole bündeln sich die Funktionen der Protokollierung. Sie ist der zentrale Baustein, in dem die Protokolldaten ausgewertet und verwaltet werden.

Die Datenschutzkonsole soll insbesondere gewährleisten, dass die *Produktion* der Protokolldaten Daten selektiv, zweckgebunden, datensparsam, verlässlich, valide und standardisiert erfolgt. Die *Auswertung* der Protokolldaten soll mit Hilfe der Datenschutzkonsole zielgerichtet, aussagekräftig und durch die Automatisierung der Prozesse effektiver erfolgen. Erst unter diesen Voraussetzungen erfüllt die Protokollierung ihre wirkliche Funktion zu dokumentieren, was der Fall ist bzw. der Fall war.

Literatur

[1] Independent Centre of Privacy Protection (ICPP) / Studio Notariale Genghini (SNG), 2003: Identity Management Systems (IMS): Identification and Comparison Study (Studie für EU), http://www.datenschutzzentrum.de/projekte/idmanage/study.htm

[3] Zu den Anforderungen an die Datensicherheit der Protokolldaten siehe Thomsen / Rost in diesem Heft.