Inhalt

DuD
Datenschutz und Datensicherheit

DuD
Datenschutz und Datensicherheit

Durch kontrollierte Protokollierung Evaluation auf Knopfdruck?

Martin Rost

Eine automatisierte Protokollierung von Ereignissen bei nahezu beliebig trimmbarer Granularität verspricht einer Organisation die Möglichkeit zu einer jederzeit möglichen Evaluierung ihrer Prozesse. Wenn eine Evaluation auf Knopfdruck jederzeit möglich wäre, dann käme dies den Anforderungen einer organisationsinternen Revision ebenso entgegen wie denen eines Datenschutzbeauftragten bzw. einer Datenschutz-Aufsichtsbehörde. Aus Datenschutzsicht muss die Protokollierung als ein eigenes Verfahren verstanden und eingerichtet werden, um eine funktionsbedingte Kontrolle der Tätigkeit insbesondere der Administration und gleichzeitig eine kontrollierte Grenze zu einer Verhaltenskontrolle der Administratoren zu ermöglichen.

Bislang werden technische Protokolldaten zumeist unkontrolliert und irgendwie erzeugt und ausgewertet. Allein was Applikationen in welchem Maße und in welcher Auflösung in Selbstauskunft über ihre soeben vollzogenen Operationen preisgeben, ist fern von jeder Qualitätssicherung, Standardisierung oder einer auch nur einigermaßen eingelebten good-practice. Dabei ist allein die bloße Speicherung von Protokolldaten in der Praxis alles andere als trivial, wie viele der Beiträge vergangener Hefte (vgl. DuD 5/2006) und speziell dieses Heftes zeigen.

Lassen sich unter diesen Bedingungen Protokolldaten zweckgebunden erzeugen und auswerten? Wie lautet die Antwort, wenn die systematische Feststellung von Störungen durch die Analyse von Protokolldaten in der Praxis nur Ausnahmefälle sind? Können Sicherheitsvorfälle gezielt analysiert werden oder erfordern sie eine Auflösung jeder Zweckbindung beim Zusammenziehen aller verfügbaren Protokolldaten, um komplexe Fehleranalysen durchführen zu können?

Jörg Apitzsch zeigt die verschiedenen Protokollierungsmechanismen von OSCI-Transport auf. OSCI-Transport gilt als derzeit praktikable Lösung für den sicheren Datentransfer über unsichere Leitungen in heterogenen Technikumgebungen unter asynchronen Bedingungen.

Vergleichbar komplex ist die Problemstellung, die *Christoph Ringelstein* in seinem Artikel bearbeitet. Ringelstein macht Vorschläge, wie Protoollierung innerhalb einer Service-Oriented-Architecture (SOA) als Infrastruktur-Dienstleistung einrichtbar wäre, und zwar so, dass Datenschutzanforderungen über mehrere Prozesse hinweg und unter Beteiligung rechtlich autonomer Organisationen eingelöst werden.

Allerdings sollten zur Protokolldatengenerierungc keine Windows-Systeme zum Einsatz kommen. *Richard Marnau* hat nämlich die Protokollierungsmechanismen unter Vista einem ersten prüfenden Blick ausgesetzt und festgestellt: Es ist wie unter Windows 2003 Server immer noch trivial möglich, die Versprachlichung der Kernelmeldungen in der Ereignisanzeige durch Manipulationen der entsprechenden DLL zu fälschen. Immerhin bietet Vista nun die Möglichkeit, Protokolldaten auf einen anderen Rechner zu transferieren, womit ein erster Schritt in Richtung einer verläßlicheren Protokollierung gewonnen ist.

Stephen Wolthusen schildert ein Konzept, mit dem sich ein Rechner auf der Grundlage von zumindest zwei CPUs selber beobachten und melden kann, wie wahrscheinlich eine Kompromittierung ist. Dadurch lässt sich die Verlässlichkeit einer Statusauskunft eines Rechners auf der Basis seiner Protokolldaten einschätzen.

Ähnlich grundsätzlich wie Wolthusen zur Technik setzen die Überlegungen von *Martin Rost* zur Funktion der Protokollierung in Organisationen an. Über Protokolle managen Organisationen ihre Beobachtungen im Hinblick darauf, was der Fall ist und was dahinter steckt. Inwieweit kann eine Zweckbindung der notorisch fehlerträchtigen Protokolldaten im Rahmen des Prozessmanagements erreicht werden? Er kommt zum Ergebnis, dass keine allzu großen Hoffnungen an deren Zweckbindungsfähigkeit geknüpft werden sollten.

Einen Überblick über die inzwischen allseits etablierten Prozessmanagementparadigmen wie ITIL und CoBIT und deren Protokollierungs- bzw. Revisionsprozesse gibt der Artikel von *Martin Meints/ Sven Thomsen*. Sie zeigen einige Revisionsstandards auf, wobei der Aspekt der Protokollierung insbesondere des omnipotenten Systemadministrators als besonders dringlich zu lösendes Problem in diesen Standards erstaunlicherweise bislang nicht die gewünschte Aufmerksamkeit erhält.

Peter Wedde stellt in seinem Beitrag fest, dass Protokollierung bzw. der Umgang mit Protokolldaten in Bezug auf Arbeitnehmer dann weitgehend unproblematisch ist, wenn alle datenschutzrechtlichen Vorgaben umfassend eingehalten werden. Kommt es allerdings in Einzelfällen zu unzulässigen Verarbeitungen oder Nutzungen automatisiert erfasster Daten, müssen Betroffene ihre Rechte individuell durchsetzen. Der Beitrag unterstreicht erneut die Dringlichkeit eines regulierten Arbeitnehmerdatenschutzes.

Kritisch diskutiert *Dirk Fox* das „Protokollierungsdilemma“ am Beispiel der Eingabekontrolle als sinnvolle Funktion einerseits sowie überzogenen Anforderungen und Datenfriedhöfen andererseits. Dies lenkt die Aufmerksamkeit wieder auf die Fragestellung, wie die Granularität bei Protokolldaten zu bestimmen ist.

Johann Bizer formuliert die Notwendigkeit einer datenschutzkonformen Konzeption der Protokollierung im Zusammenhang mit dem Selbstverständnis, den Datenschutz als eine Gestaltungsaufgabe zu interpretieren. Dabei zeigt sich, dass die datenschutzrechtlichen Anforderungen an die Protokollierung datenschutzrechtlich längst normativ formuliert sind. Sie bedürfen lediglich der Umsetzung.