

Organisationsinterne Protokollierung – Das schwierige Spiel mit dem Feuer

Martin Rost

Für Datenschützer ist das Thema automatisierte Protokollierung heikel. Denn Maschinen geben darin Auskunft über die Tätigkeiten von Menschen. Das Thema Protokollierung lässt sich jedoch in ein sicheres datenschutzrechtliches Fahrwasser führen, wenn sich die Argumentation an der „Organisationsgrenze“ orientiert. Was ist damit gemeint?

Die Kommunikationen bzw. Tätigkeiten einer *organisationsexternen Klientel* (Bürger und Kunden) darf zunächst einmal nicht personenbezogen protokolliert werden. Geschieht dies dennoch, muss der Zweck eng umrissen sein, indem er entweder hoheitlich begründet ist oder im Interesse und mit Einverständnis des Kunden vertraglich erfolgt. Anders sieht die rechtliche Situation bei der Protokollierung *organisationsinterner Mitarbeiter* aus. Hier ist in vielen Fällen eine automatisierte Protokollierung gesetzlich vorgeschrieben. Die gesetzlichen Anforderungen werden vor dem Hintergrund formuliert, die tatsächlich gegebene Zweckgebundenheit der Mitarbeitertätigkeiten – und dadurch die der Organisation insgesamt – gegenüber der externen Klientel prüfen und gegebenenfalls korrigieren zu können. Gleichwohl beanspruchen Mitarbeiter ebenfalls einen spezifisch auf ihre Belange zugeschnittenen Arbeitnehmerdatenschutz. Somit geraten zwei Datenschutzerfordernisse in eine Konfliktlage.

Die Regelungen zur organisationsinternen Protokollierung bestehen schon relativ lange. *Nils Leopold* und *Johann Bizer* diskutieren in ihren Beiträgen die gegenwärtige rechtliche Situation. *Holger Brocks* und *Heiko Behrendt* geben beispielhaft Einblicke in die gegenwärtige Protokollierungspraxis der öffentlichen Verwaltung.

Protokollierung

Aus technischer Sicht ist der Umgang mit automatisiert erzeugten Protokolldaten allerdings notorisch unzuverlässig. Denn Protokolldaten, die eine verlässliche Auskunft darüber geben können sollen, zu welchem Zeitpunkt welche Operation von welchem Mitarbeiter oder welcher Maschine ausgeführt wurden, lassen sich zwar leicht erzeugen, aber ebenso leicht auch verändern, unterdrücken oder löschen. Zugleich werden Protokolldaten nur selten dauerhaft und methodisch zu Kontrollzwecken, etwa im Rahmen einer Auftragsdatenverarbeitung bzw. des Outsourcing, ausgewertet, wenn die Systeme und Verfahren erst einmal einwandfrei zu funktionieren scheinen.

Stephen D. Wolthusen zeigt in seinem Beitrag die schnell erreichten Grenzen der Verlässlichkeit der aktuell eingesetzten Betriebssysteme für Server auf. Mit einem kurzen Seitenblick auf militärische Anforderungen wird zudem offenbar, dass das eigentliche Ziel der Protokollierung, radikal zu Ende gedacht, nur darin bestehen kann, Aktivitäten von Maschinen und Mitarbeitern möglichst ohne Zeitverzug auf sich abzeichnende Fehler zu prüfen, um diese vielleicht gerade noch rechtzeitig vermeiden zu können.

Dass von beweisfestem oder reversionssicherem Protokollieren bei Windows-Servern keine Rede sein kann, zeigt der Beitrag von *Richard Marnau*, der die aktuell verfügbaren Protokollierungsmechanismen beschreibt. Schiebt man diesen Systemen bspw. eine andere DLL-Datei unter, hat man volle Kontrolle über die Vertextung der Protokollmeldungen. *Martin Seeger* stellt anschließend die Unzulänglichkeiten des unter Unix traditionell eingesetzten *syslog*-Daemons vor und berichtet von weiterführenden Vorschlägen zur Standardisierung besser auswertbarer Logmechanismen.

Konzeptionelle Lösungen

Diese Ausführungen leiten über zu der Frage: Wie können erste pragmatische Lösungen zur Verbesserung der operativen Protokollierungsproblematik aussehen? *Sven Thomsen* und *Martin Rost* präsentieren einige konzeptionelle Überlegungen für den Betrieb eines dedizierten Protokollservers. Zwei der in diesem Beitrag entwickelten Leitlinien lauten: Protokolldaten weg von den Produktionsmaschinen! Und: Keinen Protokolleintrag ohne Zweckbindung!

Dass Protokolldaten nicht gleich Protokolldaten sind, darauf machen *Christiane Coenen* und *Ulla Dreger* aufmerksam. Sie geben einen Einblick in die verschiedenen Protokolldatentypen, wie sie bei einem Dokument-Management-System anfallen können. An diesem Beitrag lässt sich die Richtung der Entwicklung der Protokollierung ablesen:

Protokollierungsdaten lassen sich als Kennzahlen zur weit gehend automatisierten Selbststeuerung von Organisationen nutzen. Und das hat Folgen für die Überwachung von Mitarbeitern. Es wird deshalb im Zuge der Umsetzung von E-Government-Projekten zu den vornehmsten Aufgaben der Datenschützer zählen, die Nutzung dieser Daten zur Leistungs- und Verhaltenskontrolle zu verhindern.

Als Fazit dieser Beiträge muss für das Design der Protokollierung die folgende Leitlinie gelten: Protokolleinträge müssen zuverlässig und an den Problemen orientiert ausgewertet werden können, datenschutzgerecht gestaltet und verwaltet sowie sicher (d.h.: verfügbar, vertraulich, integer, authentisch) transferiert und gespeichert werden können.