DuD
Datenschutz und Datensicherheit

Funktion und Zweck des Protokollierens

Zur Zweckbindungsfähigkeit von Protokolldaten

Martin Rost

Protokolle enthalten Daten von und für Beobachtungen. Mit dem Gestalten der Protokollierung betreibt man deshalb Beobachtungsmanagement, also das Kerngeschäft des Datenschutzes. Somit stellt sich beim Domestizieren von Protokolldaten die Frage, wie es um deren Zweckbindungsfähigkeit bestellt ist.

Martin Rost

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

E-Mail: martin.rost@datenschutzzentrum.de

Einleitung

Ich möchte Sie darum bitten, werte Leserin oder werter Leser, vor dem Weiterlesen dieses Artikels darüber nachzudenken, in welchem funktionalen Verhältnis Beobachtung, Steuerung und automatisiert erfolgende Protokollierung für Organisationen aus Ihrer Sicht stehen, um abzuschätzen, ob Zweckbindungen für Protokolldaten und deren Auswertung realistisch eingefordert und umgesetzt werden können.

Bitte protokollieren Sie das Ergebnis Ihres Nachdenkens in wenigen Stichworten und vergleichen Sie diese dann mit den Vorschlägen des nachfolgenden Textes. Auf diese Weise lassen sich nicht nur Bestätigungen ihrer und meiner Vorstellungen finden, sondern auch die Störungen, die der Text in Ihrem Verständnis erzeugt, möglicherweise dadurch produktiv wenden, indem sie als kontrollierte Abweichungen von ihren Notizen, und nicht als bloßes Unverständnis, von dem Sie nicht wissen ob es zu meinen oder Ihren Lasten geht, verbucht werden. Sie merken, ich führe mit der Aufforderung zur Protokollierung Ihrer eigenen Gedanken eine Selbstbezüglichkeit ein. Beim tieferen Einstieg in das Thema „Protokollierung“ stößt man häufig auf für logische Unruhe sorgende Selbstbezüglichkeiten, die man dann arrangieren muss.

1 Protokollierungsfunktion

Die Funktion des Protokollierens auf der Ebene von Organisationen besteht, zunächst als einen abstrahierten Gesamtprozess innerhalb einer Organisation betrachtet, darin, *Beobachtbarkeit durch Sichtbarmachung einzelner Prozesse her- und bereitzustellen*. Nicht die Ergebnisse der Prozesse, sondern die Ergebnisse bzw. Produkte erzeugenden Prozesse gilt es beobachtbar zu machen.

In diesem Artikel soll deshalb die Beobachtbarkeit in der Organisation, für die Organisation sowie für andere, externe Organisationen („Aufsichtsbehörden“) thematisiert werden.

Protokolle machen Beobachtungen einer Organisation explizit, kommunizierbar, entscheidbar, formbar. Dabei bezeichnet Beobachtung eine „Bezeichnung eines Unterschieds“ (Niklas Luhmann). Die Installation einer intelligenten Organisation von trennscharfen Beobachtungen steht somit unter der Maßgabe, welche Unterschiede organisationsintern und –extern zu beobachten angemessen ist und wie diese Beobachtungen verlässlich, wirtschaftlich und rechtlich einwandfrei – heutzutage bedeutet das: automatisiert – einzurichten und skalierbar zu messen sind.

Beobachtungen sind Voraussetzungen für eine auf Kontrolle bzw. Kontrollierbarkeit aufsetzende Steuerung. Die Funktion der Kontrolle besteht darin, eine Organisation in die Lage zu versetzen, sich durch Selbststeuerung flexibel auf verschiedene Umweltbedingungen einzustellen.[1]

Kontrolle bezieht sich immer auf Prozesse, die absehbar störungsanfällig sind. Regelungstechnisch erfolgt Kontrolle entweder durch Gegen-, Rück- oder Mitkoppelung des Outputs auf den Input. Eine Organisation steuert über eigens installierte Prüfpunkte ihre kontrollierten Prozesse so an, dass diese Prozesse ihren Ist-Zustand messen und auf den voreingestellten Soll-Wert beziehen, also einen *Soll-Ist-Abgleich* vornehmen. Ein solcher Abgleich ist, wenn er in geregelten Bahnen geschieht, als Gegensteuerung eingerichtet: Kommt am Ausgang zuviel heraus, wird der Eingang verkleinert; kommt nach einem Prozess

[1] Einstellen bedeutet nicht nur Anpassen an, sondern auch Ausüben von Druck auf die Umwelt.

zuwenig heraus, wird am Eingang mehr hineingelassen. Was dabei jeweils als Zuviel oder Zuwenig zu gelten hat, stellt die als prozess-extern geltende Steuerungsinstanz ein. Störungen innerhalb der Grenzen des Zuviel oder Zuwenig können „weggeregelt" werden, sind als Störungen nicht mehr erkennbar, was sich im Nachhinein wiederum als Problem herausstellen könnte. Typischerweise führt eine erhöhte Kontrolldichte zu einer erhöhten Devianz. Ein einmal eingestellter Prozess funktioniert fortan innerhalb der Grenzen erwartungsgemäß und entspricht dem Ideal sowohl einer trivialen Maschine als auch einer Verwaltungsorganisation als auch eines Mitarbeiters, der sich an eine Aufgabenerledigung entsprechend dem Geschäftsverteilungsplan hält. Die *Prüfpunkte* für diese Kontrollen können Protokolldaten sein, die als key performance indicators (*kpi*) bezeichnet zur Vermessung von Prozessen genutzt werden.

2 Protokollierung, Monitoring und Konzeption

Wenn eine Organisation einen Abgleich von Ist- und Soll-Zuständen vornimmt, dann wird eine unmittelbare, also quasi-synchrone Beobachtung von Prozessen als *Monitoring* bezeichnet. Dieses Monitoring von Maschinen, (Sub-)Organisationen und nicht zuletzt Personen ist auf eigens dafür konstruierte und installierte Instrumente angewiesen, die eine Auswertung möglich machen.[2]

Wenn ein Abgleich von aktuellen Soll mit vergangenen Ist-Werten geschieht, dann wird dieser als Auswertung von Protokolldaten bezeichnet. Somit bezeichnet *Logging* oder *Protokollierung* eine Niederschrift (Dokumentation) von Ist-Werten für einen zukünftigen Abgleich mit Soll-Werten.[3]

Wenn ein Prozess für einen zukünftigen Soll-Ist-Abgleich entworfen wird, so wird dieser als *Systemkonzeption* oder als Systemdesign bezeichnet. Ein laufender Prozess oder eine implementierte Technik lassen sich als die Materialisierung eines Systemkonzepts auffassen. Ein Systemkonzept legt fest, welche Störungen tolerabel (also: keine) sind; welche technischen Störungen organisatorisch abgefangen werden und für die Organisation dann ebenfalls keine sind, weil ein definierter Prozess abläuft; welche Störungen dagegen zur Alarmauslösung führen, weil keine durchgeplante Ausnahmebehandlung als regulär aufgesetzter Prozess greift; und welche Ausnahmen schlicht out-of-scope sind.

All diese Fälle arrangieren die gleichen drei Komponenten, nur mit unterschiedlichen Bezügen zur Zeit: Bestimmt werden die Quelle (*Entität)* einer Aktivität, die entweder zu einem bestimmten *Zeitpunkt* oder in einer relativen Abfolge zueinander ihre Aktivität (*Operation*)

- zukünftig kontrolliert entfalten soll („Konzeption"); oder
- soeben entfaltet („Monitoring"); oder
- in der Vergangenheit entfaltete („Protokollierung").

Der allgemeine Zweck besteht so gesehen über alle drei Fälle hinweg darin, durch kausale Koppelung von Entitäten und deren konstruierbaren bzw. messbaren Operationen zu steuern oder Steuerbarkeit herzustellen.[4] Keine Organisation kann im Hinblick auf den Erhalt oder gar Ausbau von Steuerungsfähigkeit auf dieses Arrangement von Beobachtung, reproduktiver Herstellung von Kontrollierbarkeit anhand von Protokollierungsdaten an Prüfpunkten verzichten.

Es ist deshalb auch kein zufälliger Zusammenhang, dass Datenschutzgesetze bei der Verarbeitung personenbeziehbarer Daten auf die Explikation sowohl der Konzeptionen (Organisationsstruktur, IT- und Sicherheitskonzeptionen) als auch der Gestaltung der automatisierten Beobachtungen von Aktivitäten bzw. Verhalten durch Protokollierung und Monitoring besonderen Wert legen. Dadurch werden Datenschutzinstitutionen ihrerseits Teil eines umgreifenden gesellschaftlichen Regelungszusammenhangs, der steuernd Einfluss auf die Soll-Wert-Einstellungen und Ist-Messungen bei Organisationen nehmen. *Datenschutzinstitutionen sind so gesehen die gesellschaftlichen Protokollierungsinstanzen sowohl zur Feststellung des normalen Regelbetriebs als auch der Abweichungen in Bezug auf den Umgang mit personenbeziehbaren Daten durch die Organisationen der Gesellschaft*.

3 Protokollzweck

Der Zweck des Protokollierens eines einzelnen Prozesses innerhalb einer Organisation besteht darin, diesen Prozess meist anhand dessen Daten erzeugenden Operationen zu beobachten oder beobachtbar zu machen, um Abweichungen zu analysieren oder gegenwärtig zu erkennen und bei Abweichungen durch steuernde Eingriffe zukünftig zu vermeiden.

3.1 Reaktionen

Die Auswertung von Protokolldaten ist eine nochmalige Beobachtung von bereits erfolgten Beobachtungsdaten. Diese Auswertung entspricht wiederum einem Monitoring von Protokolldaten. Dieses Monitoring setzt eine eigens eingerichtete Instrumentierung[5] voraus, die hilft, diese Daten verständlich aufzubereiten, damit Prozessverantwortliche ihre Prozesse tatsächlich kontrollieren und verantworten können.[6] Auch bzw. gerade die Auswertung von Protokolldaten ist insofern als ein kontrollierter bzw. kontrollierbarer Prozess aufzusetzen, der – seinerseits anhand von Protokolldaten – zu steuern ist. Insofern machen Protokolle Beobachtung und Beobachtbarkeit transparent und reflexiv, so dass sich im Rahmen einer Protokollierung der Aktivitäten einer Organisation unabweisbar immer wieder die gleichen Fragen stellen: Was wird wie beobachtet bzw. was soll wie beobachtet werden? Enger gefasst: Wird das Wesentli-

[2] Oftmals kürzt ein selbst attestiertes „gutes strategisches Näschen" des Vorstandsvorsitzenden oder des Leiters einer Behörde die Instrumentierung für Prozesse und deren Auswertung versuchsweise ab.

[3] Der Abgleich von Soll-Werten, die in der Zukunft liegen, mit den dokumentierten Ist-Werten in der Vergangenheit verlangt Aufmerksamkeit daraufhin, auf welche Soll-Werte referenziert wird: Auf diejenigen, die zum Zeitpunkt der Ist-Wert-Feststellung galten oder hätten gelten soll oder die erst zum Zeitpunkt der aktuellen Auswertung gelten? Aus der Zukunft heraus kann grundsätzlich immer in der Vergangenheit eine Abweichung konstatiert werden, die damals festzustellen nicht möglich war.

[4] Steuern bezeichnet, im Unterschied zu einer Regelung, die gerichtete Beeinflussung eines Systems von Außen. Bei einem Regelungssystem gelingt der Ausweis einer kausal zurechenbaren Steuerungsinstanz nicht mehr: Ob der Thermostat die Raumtemperatur bestimmt oder die Raumtemperatur den Thermostaten ist bekanntlich nicht entscheidbar.

[5] Vgl. „Datenschutzkonsole", DuD 2006/05.

[6] Eine händische Protokollierung struktureller Eingriffe z.B. durch einen Systemadministrator ist, im Vergleich zu einer automatisierten Protokollierung, möglicherweise weniger zuverlässig. Allerdings steigert eine händische Protokollierung in der Regel die Chance, dass ein Fachverfahrensbetreiber tatsächlich verstehen könnte, für welchen Eingriff er die Verantwortung übernimmt.

GENUA: 1/3 Seite quer (Maße: 187 x 80 zzgl. Abstände); rechte Seite

che in angemessener Auflösung erfasst und dadurch kontrolliert beobachtbar? Noch enger gefasst: Wird eine skalierbare Ausprägung eines wesentlichen Unterschieds hinreichend genau, und dann auch: korrekt, gemessen und trifft die Bezeichnung dieses Unterschieds auf der semantischen Ebene zu? Stimmen die Protokolldaten? Und stimmen die Folgerungen, die aus der Analyse von Protokolldaten getroffen werden?

Die Auswertung von Protokolldaten geschieht unter der Fragestellung, ob *Normalbetrieb oder eine Abweichung* einst vorlag oder jetzt vorliegt. Wird keine Abweichung festgestellt, kann alles weiterlaufen wie bisher.[7] Mit der Feststellung einer Abweichung gilt es zu entscheiden, um welche Art einer Abweichung es sich handelt: Eine kleine Störung („Incident"), ein größeres Problem oder gar eine mögliche Organisationsgefährdung. Entsprechend dieser Feststellung sind die Steuerungsstrategien auszulegen.

Bei einem Incident muss möglicherweise nur ein Subprozess gestartet werden („nach einem gemeldeten Druckerausfall Drucker tauschen"). Insofern ist eine technische Störung keine organisatorische. Bei einer echten Störung des Betriebs („Die Urlaubsvertretung für den Drucker-Administrator ist ebenfalls nicht verfügbar." – eine technische Störung lässt einen organisatorischen Mangel erkennen) muss dagegen ein Soll-Wert innerhalb des bestehenden Prozesses neu eingestellt werden. Dabei gilt, nicht in die Begrenzungen des Alarmismus – vor lauter Alarmmeldungen nimmt diese niemand mehr Ernst – oder der Ignoranz – eine Katastrophe im Sinne eines point-of-no-return wird oder wurde nicht wahrgenommen – zu geraten.

Bei einem Problem stellt sich dagegen die Frage, ob zur nachhaltigen Behebung einer Störung der Prozess insgesamt zu verändern ist und Subprozesse zukünftig anders eingerichtet werden sollten. Mit Folgen für die Protokollierung: Stimmen die verschiedenen Abstimmungen von Soll- und Ist-Werten noch? Kann die Auflösung der Beobachtungen verbessert werden? Ist der Prozess der Festlegung der Soll-Werte angemessen eingerichtet („Muss die Organisation, die z.B. den Druckeraustausch konzipierte, anders eingerichtet werden? Warum wurde das Vertretungsvertretungsproblem nicht generisch geregelt? Muss das Controlling dieser Organisation neu zugeschnitten werden?").

Bei einer Störung, die im Rahmen des Changemanagements zu regulieren ist, stellt sich die Frage, ob die gesamte Prozesslandschaft der Organisation angemessen ausgelegt und Prozesse untereinander hinreichend stimmig aufeinander bezogen sind. Und in Bezug auf Protokollierung: Stimmt unsere Beobachtungssensorik, stimmen unsere Beobachtungsprozesse und unsere Auswertungsinstrumente? Erkennen wir mit diesen, ob ein vorhandener Prozess gestoppt und von einem anderen ersetzt werden muss („Können wir Hardware-Wartung und -Service outsourcen?"). Sollte womöglich ein Prozess neuen Typs eingerichtet werden (bspw. ein kontrollierter Datenschutzmanagementprozess)?

3.2 Eingriffe

Diese unterschiedlichen Prozesse zur Regulation von Störungen verlangen unterschiedliche Steuerungseingriffe innerhalb einer Organisation, was wiederum die Einrichtung unterschiedlicher Beobachtungsebenen erfordert. Auf der Ebene kleiner operativer Störungen, die nicht als organisatorische Störungen durchschlagen, spielen das Monitoring (der Loggingdaten) von einzelnen Rechnern und Applikationen, oder auf einer anderen Ebene die Aktivitäten eines Service-Desk oder die Beobachtung eines Kundenraums eine Rolle. Es gilt, Beobachtungen in kontrollierte Aktivitäten umzuleiten. Hierbei geht es um die Kontrollierbarkeit und Einrichtung der Parameter von Subprozessen innerhalb eines abgestimmten Workflows.

Für das Problemmanagement werden typischerweise mehrere von aktuellen Beobachtungen sowie falls vorhanden die technischen Protokolldaten (man denke an Festlegungen in Nutzungsbestimmungen, Dienstvereinbarungen oder Notfallplänen, die man wiederum als Protokolle der Konzeptionsfähigkeit in der Vergangenheit einer

[7] Wobei ein Ausbleiben von Abweichungen für sehr lange Zeit ebenfalls als ungewöhnlich und somit als Abweichung zu bewerten wäre.

Organisation lesen kann) herangezogen und zusammen ausgewertet, um im Rahmen der Ursachenforschung eine Kausalkette über mehrere (Sub-)Prozesse herzustellen.

Dabei kann herauskommen, dass etwas als Ursache für das Problem einschließlich der Problembehebung identifiziert gilt. Es kann aber auch herauskommen, dass die bisherigen Mechanismen der Beobachtung und Steuerung zur Aufklärung und Behebung nicht hinreichen. Gerade diesen Prozess gilt es zu protokollieren, weil dies ein Fall für die Übergabe an das Changemenagement ist, von dem viel abhängt für eine Organisation.

Das Changemanagement wirkt permanent intern steuernd. Und zwar auch dann, wenn eine Organisation gemäß der internen Protokolldatenlage erwartungsgemäß funktioniert. Hier stellt sich die grundsätzliche Frage, ob der Zuschnitt der Protokollierung in Bezug auf die Gesamtorganisation überhaupt angemessen (funktional, wirtschaftlich, rechtlich einwandfrei, politisch vertretbar) ist. Das liegt daran, dass die Umwelt von Organisationen permanent turbulent ist und zu Systemumstellungen nötigt. Dazu zählen zum einen die Konkurrenz, die gesetzlichen Anforderungen, die entweder neu oder verändert oder nicht länger ignorierbar sind, politische Leitlinien und neue wissenschaftliche Erkenntnisse sowie neue Managementmethoden und Steuerungstechniken, über die die Fachzeitschriften berichten. Generell werden beständig neue Beobachtungsinstrumente, Steuerungsmechanismen und Revisionsprozesse implementiert und immer wieder neu zueinander arrangiert. Und diese müssen permanent von neuem anhand von Protokolldaten vermessen werden.

4 Was ist der Fall? Und was steckt dahinter?

> Protokolldaten sollen Auskunft geben können auf die Frage „Was ist (oder war) der Fall?“

Deshalb werden an eine Protokollierung bzw. die Qualität der „Protokoll-Rohdaten“ hohe Anforderungen in Bezug auf Relevanz (Bedeutsamkeit), Gültigkeit und Zuverlässigkeit, Integrität, Authentizität und Vertraulichkeit gestellt. Diese Anforderungen müssen vom Protokollierungsmechanismus, man denke nicht nur an eine Logdatei, sondern auch an einen Flugschreiber oder Protokollanden, sowohl bei der Erfassung (Sensorik, Objektivität eines Protokollanden) als auch beim Transferieren, dem Abspeichern als Niederschrift (angemessen auflösendes, synchrones Mitschreiben) und Lagern der Daten (Archivierung, stabiles Medium mit kontrollierter Zugänglichkeit) erfüllt werden.

Entsprechend sind Maßnahmen zu treffen, dass diese Daten somit zweifelsfrei aus der angegebenen Quelle stammen, dass der Zugriff auf diese Daten Berechtigten vorbehalten ist und dass diese Daten nicht verändert werden können, im Falle von Loggingdaten auf Servern etwa durch die allmächtige Systemadministration.[8] Die Protokoll-Rohdaten können obendrein nur so „gut“ sein, wie

- die beteiligten Applikationen in einer Prozesskette in der Lage sind, eine zutreffende und hinreichende Selbstauskunft über ihre Operationen zu geben; und/oder
- eine speziell installierte Sensorik zur Beobachtung der unabhängig von dieser Sensorik funktionierenden, externen Systeme installiert wurde, die für das Auswertungsinteresse relevante Daten liefert; und/oder
- eine spezielle Programm-Zwischenschicht die Logmeldungen der Applikationen angemessen filtert und, orientiert an explizierten Auswertungszwecken, standardisiert, weil es praktisch unmöglich ist, all die Logmeldungen der Applikationen dieser Welt semantisch und syntaktisch zu standardisieren.[9]

> Hinter der Auswertung von Protokolldaten steht dann wiederum noch eine andere Frage, nämlich: „Was steckt hinter diesen Daten im Hinblick auf…?“

Deshalb entscheidet sich erst auf dieser Ebene, ob die Daten den Qualitätskriterien der Relevanz, Gültigkeit, Reliabilität und Vollständigkeit im Hinblick auf eine spezifische inhaltliche Fragestellung genügen, die wiederum rechtlich, wirtschaftlich und funktional formuliert sind. Und an dieser Stelle entsteht dann auch der funktional zunächst berechtigte Wunsch, dass irgendwie alles irgendwie zu protokollieren ist, weil man grundsätzlich und jetzt nicht wissen kann, ob man konzeptionell und für die Zukunft an alles gedacht hat.

Diese Daten müssen sich dabei in einen kausalen Bezug zu anderen Daten setzen lassen. Als Einstieg zur Analyse von Abfolgen und möglichen Störungen oder Fehlern werden dabei typischerweise die Zeitstempel verschiedener Protokolldatensätze genommen, mit denen sich die beteiligten Prozesse identifizieren lassen. Dabei können die Prozesse etwa im Falle einer SOA auch außerhalb des eigenen Verantwortungsbereiches liegen. Eine Bezugnahme gelingt dann nur, wenn die Zeitstempel in der gesamten Prozesskette hinreichend genau und verlässlich sind. Und spätestens dann stellt sich die Frage nach der Zweckbindung von Protokolldaten.

Beide Fragen zeigen den im Wesentlichen wissenschaftlich-kritischen und methodisch-reflektierten Anspruch sowohl an die Erzeugung als auch an die Auswertbarkeit von Protokolldaten. Mit einer wissenschaftlichen, neutralen Methode lässt sich in der Kommunikation dieser Daten und deren Auswertung im Hinblick auf zugespitzte Fragestellungen die Behauptung einer den Zweifeln enthobenen Wahrheit beanspruchen.

Um die Qualität von Protokolldaten zu verbessern empfiehlt es sich zu testen. Testen bedeutet, unter kontrollierten Bedingungen Störungen im Produktivbetrieb auszulösen, die sich in den Protokolldaten wiederfinden lassen und deren Auswertung zu entsprechenden Prozessen des Incident- oder Problemmanagements führen müssen. Durch kontrollierte Tests, bei denen man weiß, was der Fall ist und was dahinter steckt, wird eine systematisch führbare Kommunikation über Abweichungen und deren Typisierungen erzeugbar. Dies wiederum könnte u.a. auch hilfreich sein, um die Zweckbindung im Umgang mit Protokolldaten zuschneiden zu können.

5 Zweckbindung?

Welche Zweckbindung von Protokolldaten kann man in diesem konzeptionellen Rahmen also fordern?

Die Protokolldaten, die die Applikationen im Zuge ihrer „Selbstauskunft“ herausschreiben oder die von einer eigens zu Protkollierungszwecken installierten Beobachtungs-Applikation herausgeschrieben werden, müssen eigentlich alle gesichtet, semantisch und syntaktisch standardisiert

[8] Vgl. zu den Anforderungen an eine revisionsfeste Protokollierung in Bezug auf Verfügbarkeit, Integrität, Vertraulichkeit, Zweckbindung und Isolation den Beitrag von Thomsen/ Rost, Zentraler Protokollservice, DuD 2006/05: 292-294.

[9] Vgl. den Beitrag von Rost/Thomsen, Die Datenschutzkonsole, DuD 2006/05: 295-297.

und entsprechend den zuvor kurz angesprochen Qualitätsanforderungen in Bezug auf Datensicherheit und Datenschutz dann produziert und gespeichert werden. Sie sollen Auskunft geben über die Aktivität einer Applikation, die insbesondere zur Analyse auf der technisch-operativen Ebene relevant sind. Sie bilden die Basis für die Dokumentation verketteter Elementaraktivitäten, auf der sich die Frage, was auf dieser Ebene der Operationen der Fall war, klären ließe. Hinter all den Aktivitäten der Maschinen und in Organisationen stehen irgendwann Menschen, die diese ausgelöst oder zu verantworten haben. Ohne eine Standardisierung der Bezeichnung von Elementarereignissen können Datensparsamkeit und Nichtzurechenbarkeit auf Mitarbeiter oder Klienten nicht ernsthaft eingefordert werden, weil diese ein Abwägen in Bezug auf einen gut spezifizierten Zweck und dessen Beschreibbarkeit voraussetzt. Im Zweifel würde somit alles protokolliert werden. Und das ist das, was derzeit ohnehin stattfindet.

Wenn das Herausschreiben von Protokoll-Rohdaten nicht sehr viel besser eingerichtet werden kann, dann stellt sich die Frage, ob man nicht zumindest die Auswertung von Protokolldaten einfacher „zweckbinden“ könnte. So wäre ja denkbar, die Protokoll-Rohdaten zu nehmen, zumindest die offensichtlich personenbezogenen Daten ohne Zweckbindung herauszufiltern und zu löschen oder zu anonymisieren, die restlichen Daten verschlüsselt abzuspeichern und zur Auswertung nur diejenigen Daten zu entschlüssen, die unter einer bestimmten Perspektive als erforderlich und zweckgemäß erscheinen.

Die Auswertung von Daten erfolgt durch Bezugnahme auf den Workflow, in den eine Applikation integriert ist. Hiernach käme eine Zweckbindung dadurch zustande, indem im Vorhinein die inhaltlichen Interessen begründet und die Auswahl der dafür relevanten Daten bestimmt werden müsste. Das sind Daten, die typischerweise das spezifikations- und rechtmäßige Funktionieren von Applikationen und Prozessen belegen sollen. Allerdings geht es bei Fehleranalysen im Rahmen des Incidentmanagement gerade darum, nichtspezifikationsgemäße Ereignisverkettungen innerhalb der Protokolldaten etwa einer Applikation aufzudecken und nachzeichnen zu können.

Es ist ein Widerspruch in sich, genau für das Nichterwartbare im Vorhinein eine Zweckbindung zu fordern, die ihren Namen auch verdient, weil sie hinreichend spezifisch formuliert wurde. Und weil eine Organisation vor der Aufgabe steht, zukünftige Fehler zu vermeiden, indem (Sub-)Prozesse in Bezug auf Soll/Ist-Konfiguration anders skalieren sollten, Prozesse vielleicht anders anzusteuern oder gänzlich zu verändern oder zu ersetzen wären, wird sie sich nicht an als unzureichend festgestellte Zweckbindungen halten. Eine Auswertung von Protokolldaten im Rahmen des Problemmanagements erzeugt zudem noch eine weitere Schwierigkeit:

Bei einer Fehleranalyse im Rahmen des Problemmanagements werden typischerweise sämtliche Protokolldaten, die eine Rolle spielen könnten, herangezogen. Dadurch sollen Ereignisketten rekonstruiert werden können, die von der Spezifikation nicht nur einer Applikation, sondern des gesamten Workflows oder einer Applikationen irgendwo in der Prozesskette abweichen. Eine Zweckbindung im Rahmen des Problemmanagement müsste darauf abzielen, im Vorhinein zu regeln, welche Protokolldatensätze von ganz unterschiedlichen Systemen, aus möglicherweise anderen (Sub-)Organisationen herangezogen und gemeinsam ausgewertet werden dürfen und welche nicht. Wieder scheint es mir unrealistisch davon auszugehen, dass eine Organisation Kontroll- bzw. Prozessgestaltungsmöglichkeiten verschenkt.

6 Fazit

In allen drei Fällen – also sowohl dem Herausschreiben von Protokoll-Rohdaten, als auch der Auswertung eines einzelnen Protokolldatensatzes sowie vieler in Bezug zueinander gesetzter Protokolldatensätze -, zeigt sich, wie schwierig es ist, Zweckbindung durchzusetzen, wenn dadurch für eine Organisation Kontroll- und Steuerungsinformationen im Rahmen des Risikomanagements verloren gehen.

Der Schlupf[10], der mit der derzeit erreichbaren Qualität von Protokolldaten und deren Auswertungsmöglichkeiten einhergeht, mag ausreichen, damit Organisationen sich selber organisieren und andere Organisationen von ihrer Zuverlässigkeit und Compliance überzeugen können. Die Qualität der Datensicherheit von Protokolldaten reicht aber nicht, um aus ihnen direkt existentielle Entscheidungen für einzelne Personen zu rechtfertigen. Und um eine wirkungsvolle Zweckbindefähigkeit von Protokolldaten ist es vermutlich ebenso schlecht bestellt.

[10] Als Schlupf bezeichnet man in der Mechanik mangelnde Präzision im Hinblick auf synchrone Rotationen, wobei dieser Mangel durchaus funktional ist bzw. der Mangel sich abstellen ließe. Der Mangel im Subsystem ist somit keiner sondern funktional für das Gesamtsystem.