

Ulrich Flegel, Oliver Raabe, Richard Wacker

Technischer Datenschutz für IDS und FDS durch Pseudonymisierung

Die Speicherung personenbezogener Daten in Intrusion Detection und Fraud Detection Systemen ist datenschutzrechtlich eine Gratwanderung zwischen Sicherheits- und Compliance-Anforderungen einerseits und klarer Zweckbestimmung sowie einem wirksamen Schutz vor unzulässiger Leistungs- und Verhaltenskontrolle andererseits. Der vorliegende Beitrag schlägt eine Lösung des Dilemmas durch Pseudonymisierung vor.

1 Einleitung

Die technische Angriffserkennung zum Schutz von IT-Systemen und die technikgestützte Betrugserkennung und –abwehr in Unternehmen können sich vergleichbarer Techniken bedienen. Beiden Systemen ist gemeinsam, dass sie neben den grundsätzlich legitimen Zwecken im Unterneh-



Dr. Ulrich Flegel

ist Wissenschaftler am Forschungszentrum Karlsruhe der SAP AG und Gastprofessor an der

Universität Mannheim
E-Mail: ulrich.flegel@sap.com



Dr. Oliver Raabe

ist als Forschungsgruppenleiter am Institut für Informations- und Wirtschaftsrecht (IIWR),

Karlsruhe Institut of Technology (KIT) mit Fragen der rechtlichen Bewertung komplexer IT-Systeme befasst.
E-Mail: raabe@kit.edu



Dipl.-Inform. Wirt Richard Wacker

Wissenschaftlicher Mitarbeiter am Institut für

Informationsrecht und Wirtschaftsrecht (IIWR), Karlsruhe Institut of Technology (KIT)
E-Mail: richard.wagner@kit.edu

men auch zur Verhaltens- und Leistungskontrolle verwendet werden können.

Vor diesem Hintergrund sollen in diesem Beitrag auf Basis des novellierten BDSG die jeweiligen Rechtsgrundlagen für die einzelnen Phasen und Ziele des Einsatzes dieser Systeme im Rahmen des informations- und kommunikationstechnischen (IKT) Sicherheitskonzeptes eines Unternehmens identifiziert werden. Im zweiten Schritt werden zu beiden Szenarien Mechanismen der Pseudonymisierung eingeführt, welche die gesetzliche Grenzziehung des jeweils legitimen Einsatzzweckes zu technisch möglichen Missbrauchsszenarien unterstützend absichern.

2 Intrusion Detection

Ein Intrusion Detection System (IDS) dient der Erkennung von Verletzungen der IT-Sicherheitspolitik in einem Unternehmen.¹ Üblicherweise erledigen Mitarbeiter eines Unternehmens geschäftliche Aufgaben mittels Rechnern, die von der IT-Abteilung der Firma installiert, gewartet und durch verschiedene technische Maßnahmen gemäß der IT-Sicherheitspolitik geschützt werden. Zu diesen Maßnahmen zählen u. a. Firewalls, Anti-Viren-Software und Zugriffsschutzsysteme.

Ein umfassender Schutz ist jedoch aus verschiedenen Gründen nicht realisierbar. Einerseits benötigen Mitarbeiter für die Erfüllung ihrer Aufgaben Freiräume, die auch den Gebrauch des Arbeitsmittels PC betreffen. So können bspw. Zugriffe eines Mitarbeiters auf solche Anwendungen und Dateien im Dateisystem technisch verhindert

werden, die dieser nicht benötigt. Missbräuchliche Aktivitäten auf Dateien und Anwendungen, die der Mitarbeiter berechtigterweise nutzt, können auf diesem Weg jedoch nicht verhindert werden. Andererseits sind auch die zum Einsatz gebrachten Abwehrmaßnahmen nicht frei von Lücken und Fehlern, die bspw. durch von Mitarbeitern fahrlässig oder vorsätzlich eingebrachte Schadprogramme ausgenutzt werden können. Diese Sicherheitslücke soll durch den Einsatz von IDS geschlossen werden.

2.1 Funktion und Aufbau eines IDS

Für die nachfolgende Analyse werden zwei Fälle betrachtet. Im ersten Fall sendet ein Mitarbeiter des Unternehmens nur für den internen Gebrauch bestimmte Dokumente an eine externe E-Mail-Adresse. Im zweiten Fall nutzt ein anderer Mitarbeiter Zugriffsmöglichkeiten auf persönliche Dokumente seiner Kollegen in versehentlich freigegebenen Verzeichnissen. Zur Erkennung solcher Angriffe nutzt das Unternehmen ein IDS mit folgendem Aufbau (siehe Abb. 1²):

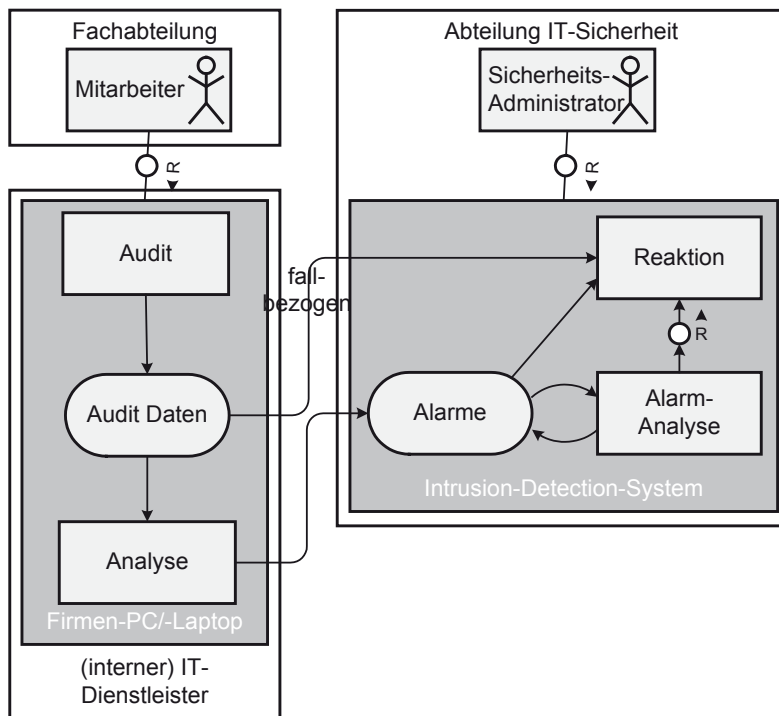
Die auf dem Rechner des Mitarbeiters befindliche *Audit-Komponente* sammelt feingranulare *Audit-Daten* über die Aktivitäten auf dem System. Diese Daten werden für mögliche Beweis Zwecke vorübergehend auf der lokalen Festplatte gespeichert und fortlaufend auf Angriffsmuster hin analysiert (*Analyse*). Ein erkanntes Angriffsmuster³ führt zu einer Alarmmeldung, die zur

² IT-Systeme werden im Folgenden in FMC modelliert. Knöpfel/Gröne/Tabeling, Fundamental Modeling Concepts: Effective Communication of IT Systems, 2006

³ Ein Angriffsmuster ist ein wiedererkennbares Ablaufschema einer sicherheitsgefährdenden Handlung.

¹ Siehe Fox, Gateway, DuD 9/2000, S. 549.

Abbildung 1 | Herkömmliche Realisierung von Intrusion Detection und Beweissicherung



Auswertung an die zentrale *Alarmanalyse* des IDS gesandt wird. Eine solche Meldung enthält Auszüge aus den Audit-Daten, welche die entdeckte Instanz eines Angriffs beschreiben. Anschließend erfolgt eine semi-automatische oder manuelle *Reaktion* durch den *Sicherheitsadministrator*.

In den oben eingeführten Beispielen würden die Zugriffe über die lokale Audit-Komponente des Mitarbeiters erfasst. Aufgrund der Prozess-ID des E-Mail-Programms und des durch diesen Prozess ausgelösten Dateizugriffs bzw. im zweiten Fall aufgrund der Pfade der Dateizugriffe würde diese regelhaft einen Alarm erzeugen, welcher im Alarmanalysesystem des zentralen IDS ausgewertet und in eine entsprechenden Reaktion münden würde.

2.2 Rechtliche Wertung

Aus rechtlicher Sicht ist zunächst die Legitimation der vorgenannten Schritte zu bewerten. Das bedeutet zunächst die richtige Rechtsgrundlage aufzufinden und anhand dieser Rechtsgrundlage das konkrete Szenario zu bewerten. Im hier betrachteten Bereich des Rechts der elektronischen Datenverarbeitung stellt allerdings schon das Auffinden des einschlägigen

datenschutzrechtlichen Regulierungsregimes nach wie vor eine bedeutende Hürde für die Rechtsanwendung dar. Neben den Regelungen des Bundesdatenschutzgesetzes können sich regelmäßig auch die spezielleren Regelungen der §§ 88 ff. TKG und 11 ff. TMG als einschlägig erweisen.

2.2.1 Anwendbares Recht

Ohne auf die grundsätzlichen Fragen nach der richtigen Abgrenzung der Regelungsbereiche zueinander vertieft einzugehen⁴ kann für die Beurteilung des vorliegenden Sachverhalts als Faustformel ein Blick auf die jeweils einschlägigen Datenkategorien und Akteure eine Zuordnung erleichtern. In dem Beispielszenario werden als Datenbasis für die nachfolgende Analyse personalisierte Zugriffe auf das Dateisystem und die verwendeten Anwendungsapplikationen erhoben und gespeichert.

Das TKG ist insofern nicht anwendbar, als der Unternehmer beim Betrieb eines lokalen Rechnernetzes im Innenverhältnis schon nicht als Diensteanbieter i.S.v. § 3 Abs. 6 TKG auftritt. Zudem weisen die fraglichen Daten keinen telekommunikationsrechtlich relevanten Bezug auf, wie es etwa bei der Protokollierung von IP-Ad-

ressen im Rahmen der Internetkommunikation oder Vergleichbarem der Fall wäre.

Die Anwendbarkeit der bereichsspezifischen Regelungen des TMG ist schon deshalb nicht gegeben, weil es sich bei dem protokollierungsrelevanten System nicht um einen Informations- oder Kommunikationsdienst i.S.v. § 1 TMG handelt. Läge ein Dienst im vorgenannten Sinne vor, fielen dieser jedoch unter die Regelung des § 11 Abs. 1 Nr. 1 TMG, welcher Dienste zur ausschließlichen Verwendung im Dienst- oder Arbeitsverhältnis von der Anwendung der den Datenschutz betreffenden Regelungen des TMG ausnimmt.

Somit verbleibt es für die Beurteilung der Datenverwendung des Beispielsachverhaltes bei der umfassenden Anwendbarkeit der Regelungen des Bundesdatenschutzgesetzes. Als Rechtsgrundlage für alle Phasen der Datenverwendung kommt damit § 4 BDSG in Betracht.

Anzumerken ist jedoch, dass dieses Ergebnis aus der spezifischen Sachlage, nicht jedoch aus der Betrachtung von IDS allgemein folgt. Es existieren viele Beispiele für IDS-Lösungen, für welche sich TM oder TK-rechtliche Normen als anwendbar erweisen würden.⁵

2.2.2 Personenbezogene Daten

Die Anwendbarkeit der datenschutzrechtlichen Normierung hängt davon ab, ob die Audit-Daten personenbezogene Daten i. S. d. § 3 Abs. 1 BDSG darstellen. Dies kann angesichts der bei Audit-Daten und Alarm-Meldungen jeweils mitgeführten und von der Unternehmung selbst vergebenen Benutzer-ID als gegeben gelten. Insbesondere durch die mögliche Zuordnung der Benutzer-ID zu Zeitstempeln und benutzten Systemkomponenten lassen sich auf Basis der zu Beweiszwecken gespeicherten Auditdaten weitgehende Verhaltensprofile des entsprechenden Mitarbeiters erstellen.

2.2.3 Erlaubnistatbestände

Im Folgenden soll erörtert werden, wie die Verarbeitung der erhobenen Daten, einerseits zum Zweck der Sicherstellung des ordnungsgemäßen Betriebs der DV-Anlage und andererseits zum Zweck der Verhaltens- und Leistungskontrolle gesetzlich be-

Vgl. Meier, *Intrusion Detection Effektiv: Modellierung und Analyse von Angriffsmustern*, Kapitel 5, 2007.

4 Vgl. Raabe/Dinger, C&R 2007, 791 ff

5 Vgl. z. B. Meier, *Intrusion Detection Effektiv: Modellierung und Analyse von Angriffsmustern*, Kapitel 3, 2007

wertet wird. Auch wenn beide Aktivitäten einer spezifischen Legitimation bedürfen, ist zunächst von der Normierung des § 4 BDSG als Rechtsgrundlage für die Verwendung auszugehen. Eine Einwilligung nach § 4 Abs. 1 (Alternative zwei) BDSG dürfte jedoch insofern ausscheiden, als bei Maßnahmen im Dienst- und Arbeitsverhältnis jedenfalls die von § 4a BDSG für die Wirksamkeit der Einwilligung vorausgesetzte Freiwilligkeit bezweifelt werden kann. Damit stellt sich die Frage nach dem Vorliegen von gesetzlichen Erlaubnistatbeständen für den jeweils verfolgten Zweck.

► Verwendung aus Gründen der IT-Sicherheit

Die zur Echtzeit-Erkennung von Angriffen auf dem lokalen System durch die Audit-Komponente notwendige Erhebung und Verarbeitung der Daten kann grundsätzlich nach § 28 Abs. 1 (Alternative zwei) BDSG als legitimiert angesehen werden.⁶ Soweit im vorliegenden Szenario auch die Verhinderung von Angriffen auf die Privatsphäre anderer Nutzer in Frage steht (vgl. zweites Beispiel), tritt möglicherweise flankierend der Auftrag einer Zugriffskontrolle nach Nr. 3 der Anlage zu § 9 Abs. 1 BDSG hinzu.

Auch das vorübergehende Speichern der Audit-Daten auf dem lokalen System des Mitarbeiters aus Gründen der Beweis-sicherung kann auf dieser Grundlage legitimiert werden.⁷ Das schutzwürdige Interesse des Nutzers ist in diesem Falle mit dem Interesse des Arbeitgebers zur Erkennung neuer Angriffsmuster aus dem Datenbestand zur Anpassung der Regelbasis der Echtzeit-Erkennung abzuwägen.

Darüber hinaus ist ein nachträgliches Audit auf den vorhandenen Daten grundsätzlich auch aus arbeitsrechtlicher Sicht relevant, da es dem beweisbelasteten Arbeitgeber sonst kaum möglich wäre, eine Verletzung der Vorgaben der IT-Sicherheit im Unternehmen zu beweisen. Allerdings ist insbesondere im Hinblick auf die Integritätserwartung des Nutzers zu berücksichtigen, ob die Nutzung des Systems auch für private Zwecke gestattet oder verboten ist.

► Verwendung zur Verhaltens- und Leistungskontrolle

Die Verwendung der lokalen Audit-Komponente zu einer Verhaltens- und Leistungskontrolle⁸ des Arbeitnehmers ist von der Erkennungspolitik der IDS-Analyse

abhängig. Theoretisch kann ein Alarmsystem auch so gestaltet werden, dass es auf (vermutlich) nicht arbeitsbezogene Aktivitäten des Nutzers reagiert, bspw. die exzessive Nutzung des Webbrowsers und dergleichen. Ebenso können die gespeicherten Audit-Daten nachträglich auf entsprechende Muster untersucht werden. Beiden Fällen ist aber mit der Regelung des § 31 BDSG, bei anfänglicher Zweckfestlegung der Datenverwendung auf die Sicherstellung eines ordnungsgemäßen Betriebes der DV-Anlage, ein rechtlicher Riegel vorgeschoben, da § 31 BDSG die Regelung des § 28 BDSG für diese Fälle verdrängt. Die zweckabändernde Nutzung zur Verhaltens- oder Leistungskontrolle ist somit unzulässig.⁹

Fraglich ist allerdings, ob dies auch zu gelten hat, wenn die Datenverwendung schon anfänglich auch zum Zwecke der Verhaltens- und Leistungskontrolle vorgesehen wurde. § 31 BDSG schließt nur eine nachträgliche Zweckänderung aus.¹⁰ Da sich die anfängliche Zweckrichtung in diesem Falle auf das Beschäftigungsverhältnis bezieht, ist auf diesen Fall, nach der Novelle des BDSG nunmehr § 32 anzuwenden welcher wiederum § 28 BDSG für seinen Anwendungsbereich verdrängt. Die Regelung selbst trägt allerdings in ihrem materiellen Gehalt nichts wesentlich Eigenständiges zur Beantwortung der Frage nach der Legitimation bei, als sie schon ausweislich der Gesetzesbegründung die von der Rechtsprechung erarbeiteten Grundsätze des Datenschutzes im Beschäftigungsverhältnis lediglich zusammenfasst.¹¹ In formeller Hinsicht ergibt sich zudem das flankierende Mitbestimmungsrecht des Betriebsrates in diesem Fall schon aus § 87 Abs. 1 Nr. 6 BetrVG, womit sodann über eine entsprechende Betriebsvereinbarung die Verwendung vorrangig legitimiert würde.

Im Hinblick auf die mögliche Echtzeitüberwachung des Nutzerverhaltens ist nach den Alternativen des § 32 BDSG eine differenzierte Wertung zu treffen. Die Bewertung richtet sich einerseits nach § 32 Abs. 1 (Alternative eins) BDSG, der grundsätzlich die Befugnisse zur Kontrolle der Leistung oder des Verhaltens des Beschäftigten terminiert.¹² Wegen der Nähe der Sachbereiche kann insofern die Recht-

sprechung und Literatur zur Kontrolle von Diensttelefonaten oder Videoüberwachung am Arbeitsplatz herangezogen werden. Die Nähe zu diesen Bereichen ergibt sich aus dem jeweiligen Echtzeitcharakter der Kommunikation. Der Bewertung kann somit nicht pauschal die Frage nach dem Verbot oder der Erlaubnis der privaten Nutzung der IKT-Infrastruktur zugrunde gelegt werden.¹³ Zwar überwiegt im Falle der Erlaubnis das Interesse des Nutzers das Kontrollinteresse des Arbeitgebers. Jedoch ist auch im Falle des Verbots der privaten Nutzung wegen des totalen Charakters der IT-Kontrolle auch das Integritätsinteresse und Vertrauen des Arbeitnehmers in den Fokus zu nehmen. So soll mit dem neuen Grundrecht zum Vertrauen in die Vertraulichkeit und Integrität informationstechnischer Systeme auch bei der geschäftlichen Nutzung von IT-Systemen jedenfalls dann eine Vertraulichkeits- und Integritätserwartung geschützt sein, wenn die selbstbestimmte Nutzung eines Systems „als eigenes“ im Fokus des Nutzers steht.¹⁴ Diese wird durch ein Verbot der privaten Nutzung bei der Echtzeit-Kontrolle nicht zwangsläufig eliminiert. Entscheidend ist vielmehr die Frage, ob die Echtzeitüberwachung einen dauernden Überwachungsdruck¹⁵ auslöst, dem sich der Betroffene nicht entziehen kann¹⁶ und der in keinem angemessenen Verhältnis zum Kontrollzweck steht. Damit ist allenfalls eine offene, stichprobenhafte Verhaltens- und Leistungskontrolle in Echtzeit zulässig.¹⁷

Hinsichtlich der Speicherung zu Zwecken der späteren stichprobenartigen Auswertung zu Zwecken der Verhaltens- und Leistungskontrolle ist in Anlehnung an die zur Kontrolle von E-Mail und Internetnutzung am Arbeitsplatz entwickelten Rechtsprechung und Literatur,¹⁸ davon auszugehen, dass dadurch das Interesse des Arbeitgebers an Kosten- und Arbeitskontrolle in verhältnismäßiger Weise realisiert werden kann. Konfliktpotential, wie es sich z. B. bei der Überwachung des dienstlichen E-Mail-Verkehrs mit dem Betriebsrat auch für den Fall des Ausschluss-

¹³ So aber wohl der Rechtsgedanke hinter § 11 Abs.1 Nr. 1 TMG und die Literatur zur Kontrolle bei der Nutzung von E-Mail am Arbeitsplatz, vgl. Stögmüller CR 2008, 437 m.W.n.

¹⁴ Stögmüller, CR 2008, S. 436

¹⁵ Zum Begriff vgl. BAG, NJW 1986, 2724.

¹⁶ Meyer, K&R 2009, 15.

¹⁷ Fußnote DSR-Grundsätze bei der dienstl./ privaten Email und Internetnutzung

¹⁸ Vgl. Stögmüller, CR 2008, S. 437 m. w. N.

⁶ Vgl. Runge, CR 1994, 713.

⁷ Vgl. Runge CR 1994, 710.

⁸ Zum Begriff vgl. Meyer, K&R 2009, S. 14

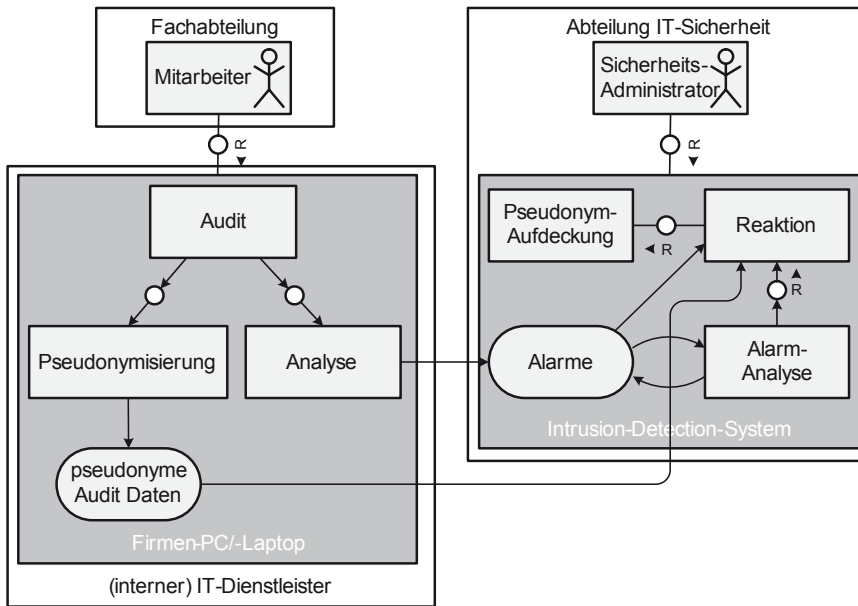
⁹ Explizit für Protokolle: Runge, CR 1994, S. 710

¹⁰ Gola/Schomerus, 9. Auflage (2007,) § 31 BDSG, RN. 5

¹¹ BTDRs. 16/13657 S. 35.

¹² BTDRs. 16/13657 S. 36.

Abbildung 2 | Speicherung pseudonymer Daten zur Beweissicherung



ses der privaten Nutzung andeutet,¹⁹ ist wegen des deutlich geringeren Inhaltsbezuges hier nicht ersichtlich. Soweit allerdings eine Aufklärung des Arbeitnehmers unterbleibt und sowohl die Protokollierung als auch die Auswertung im Geheimen stattfinden, ist nach der konkretisierenden Regelung des § 32 Abs. 1 (Alternative 2) BDSG ein zu dokumentierender hinreichender Anfangsverdacht für eine Straftat vorausgesetzt. Zudem ist zur verfahrensrechtlichen Absicherung die Beteiligung des Datenschutzbeauftragten erforderlich.²⁰

2.2.4 Datengeheimnis und Pseudonymisierung

Aus rechtlicher Sicht ist der Einsatz von IDS sowohl zur Missbrauchsabwehr als auch in Grenzen zur Verhaltens- und Leistungskontrolle zulässig. Problematisch ist allerdings, dass diese gesetzliche Grenzziehung in dem hier beschriebenen System nicht durch absolut wirkende technische Mechanismen vor vorsätzlich rechtswidrigem Verhalten geschützt ist. Da die notwendigen Analysen auf Klardaten durchgeführt werden, besteht weiterhin ein Missbrauchsrisiko, denn grundsätzlich können die ursprünglich nur zu Zwecken des Beweises (§ 31 BDSG Verbot der Zweckänderung) im Rahmen der IT-Sicherheitskontrolle erhobenen Daten

nachträglich zur Leistungskontrolle umgewidmet werden.

Auch wenn mit der Novelle des BDSG der Normappell des § 3a BDSG nicht verändert wurde, so ist als flankierende Maßnahme insofern gleichwohl das Gebot der Nutzung von Techniken der Pseudonymisierung noch einmal gestärkt enthalten. Daher soll im Folgenden ein Ansatz²¹ vorgestellt werden, welcher durch Verwendung von Pseudonymen einen verbesserten Schutz der gesetzlichen Grenzziehung ermöglicht, ohne die bestimmungsgemäße Funktionalität des Systems einzuschränken.

3 Pseudonymisierung für IDS

Durch die hier vorgeschlagene Pseudonymisierung tritt an die Stelle der organisatorischen Einschränkung des Zugriffs auf die zulässigerweise gespeicherten Klartext-Audit-Daten die Möglichkeit des ständigen uneingeschränkten Zugriffs auf pseudonymisierte Audit-Daten. Hierzu muss die Pseudonymisierung folgende Anforderungen erfüllen²²:

- ♦ **Vertraulichkeit:** Durch die Pseudonymisierung werden sensitive und personenbezogene Daten geheim gehalten. Sie dürfen daher an keiner Stelle des Verfahrens mit explizitem oder leicht

wiederherstellbarem Personenbezug gespeichert werden, so dass die Pseudonymisierung umgangen wird. Zudem muss die Vertraulichkeit der Pseudonym-Zuordnungsregel geeignet sichergestellt sein.

- ♦ **Verkettbarkeit:** Die pseudonymisierten Daten müssen ebenso effektiv wie die Originaldaten auf Angriffe analysierbar sein. Es muss daher ein Weg gefunden werden, die analyserelevanten Beziehungen zwischen Audit-Daten-Merkmalen zu erhalten.
- ♦ **Technisch zweckgebundene Zurechenbarkeit:** Für Angriffsszenarien die auf organisatorisch abgestimmten Mustern beruhen, sollte die Pseudonymisierung technisch aufgedeckt werden, um eine Überforderung²³ der organisatorisch zweckgebundenen Aufdeckung zu vermeiden.
- ♦ **Organisatorisch zweckgebundene Zurechenbarkeit:** Für Angriffsszenarien, welche keinem bekannten Muster entsprechen, soll eine Aufdeckung ebenfalls möglich sein. In diesem Fall muss eine organisatorische Sicherstellung der Zweckbindung durch technische Mittel durchgesetzt werden.²⁴

3.1 Erfüllung der Anforderungen

Audit-Daten, welche in einem IDS gespeichert werden, sind, bezogen auf das eingangs geschilderte Beispiel, Ereignis-Typ, Zeitstempel, Rechnername, Benutzer-ID und der Name des/der auslösenden Programms/Systemkomponente. Unter diesen sind jedenfalls die Benutzer-ID, möglicherweise auch die Rechner-ID und weitere als die Person bestimmende Merkmale zu werten. Ein technisches Verfahren, welches den Personenbezug der Audit-Daten beseitigt, muss somit mindestens dieses Merkmal durch ein nicht zuordenbares Pseudonym ersetzen.

Abbildung 2 stellt eine Weiterentwicklung des herkömmlichen IDS dar, welches sich durch die an die *Audit*-Komponente angebundene *Pseudonymisierung* unterscheidet. Auf dem System des Mitarbeiters werden weiterhin *Audit-Daten* gesammelt, aber in diesem Fall ausschließlich

²³ Durch eine solche Überforderung müsste die Schwelle zur Aufdeckung aufgrund der begrenzten Zeit der Beteiligten zulasten der Systemsicherheit unverhältnismäßig hoch angesetzt werden.

²⁴ Z. B. über Schwellenwert-Kryptosysteme, vgl. Gemell, An Introduction to Threshold Cryptography, In: Cryptobytes Vol. 2, Nr. 3, S. 7, 1997

¹⁹ Schild/Tinnefeld, DuD 2009, S. 472

²⁰ Schild/Tinnefeld, DuD 2009, S. 473

²¹ Flegel, Privacy-Respecting Intrusion Detection, Part 2, 2007

²² Flegel, Datenschutzfreundliche Missbrauchsentscheidung, Digma 5(4) S. 168-171, 2005

pseudonymisiert auf der lokalen Festplatte gespeichert.²⁵ Führt die lokal durchgeführte Analyse der Daten zu einem Alarm, so kann der Sicherheitsadministrator die Alarmbeschreibung und Daten aus der pseudonymisierten Datenbasis des lokalen Rechners zur genaueren Untersuchung einsehen.

Bestätigt sich der Verdacht eines Angriffs, können die Pseudonyme unter bestimmten Voraussetzungen aufgedeckt und die Daten zu Beweis Zwecken offengelegt werden. Die Einzelschritte der Pseudonymisierung werden im Folgenden technisch detaillierter beschrieben.

3.1.1 Vertraulichkeit und Verkettbarkeit

Im ersten Schritt werden durch den Pseudonymisierer alle personenbezogenen Merkmale durch ein Pseudonym ersetzt und das Originalmerkmal mittels eines symmetrischen Verschlüsselungsverfahrens²⁶ auf Basis eines hinreichend langen, zufällig gewählten Schlüssels k verschlüsselt. Unter der Voraussetzung, dass k dem Angreifer unbekannt ist, wird hierdurch eine Rückgewinnung praktisch unmöglich. Die analyserelevanten Beziehungen der Audit-Daten-Merkmale untereinander bleiben entweder durch Beibehaltung der Merkmale im Klartext oder durch entsprechende verkettbare Wahl der Pseudonyme (Anforderung 2) erhalten.

3.1.2 Technisch zweckgebundene Zurechenbarkeit

Ein bekanntes Angriffsmuster umfasse mindestens n verschiedene Einzelaktionen. Der Schlüssel k der zur Chiffrierung des Personenbezuges verwendet wurde, wird in n oder mehr Schlüsselanteile zerlegt und jeder Einzelaktion ein eigener Schlüsselanteil zugeordnet. Hierzu wird ein informationstheoretisch sicheres Verfahren²⁷ genutzt, welches gewährleistet,

dass der Schlüssel k nur dann effizient berechenbar ist, wenn mindestens n Schlüsselanteile bekannt sind. Mit jeder Einzelaktion, die tatsächlich vom Nutzer ausgeführt wird, erhält der Sicherheitsadministrator einen Schlüsselanteil des Schlüssels k . Sobald das bekannte Angriffsmuster vollständig vom Nutzer ausgeführt wurde, kann folglich der Schlüssel k effizient berechnet und damit der Personenbezug der Daten wieder hergestellt werden.

3.1.3 Organisatorisch zweckgebundene Zurechenbarkeit

Ein ähnliches Verfahren wird für die organisatorisch zweckgebundene Zurechenbarkeit (Anforderung 4) angewandt. Hierzu muss vorab eine Festlegung getroffen werden, welcher Personenkreis an der Aufdeckung eines Pseudonyms ohne Hinweise auf ein bisher bekanntes Angriffsmuster beteiligt werden soll. Anschließend wird der Schlüssel k in entsprechend viele Schlüsselanteile zerlegt, wobei diese vertraulich an die festgelegten Personen verteilt werden. Eine Entschlüsselung der Daten und damit die Wiederherstellung des Personenbezugs sind dann nur möglich, wenn diese Personen unter Verwendung ihrer Schlüsselanteile zusammenwirken.²⁸

3.1.4 Vertraulichkeit der Pseudonym-Zuordnungsregel

Die Pseudonymisierung der Daten ist der Speicherung vorgelagert. Ohne einen Angriff auf die Integrität der Pseudonymisierung können die Ursprungsdaten nur durch die technische oder organisatorische Aufdeckung im Einzelfall zurückgewonnen werden. Die Pseudonymisierung wie auch das lokale Audit finden unter der Hoheit des IT-Dienstleisters außerhalb des Einflussbereichs der Sicherheitsadministratoren statt. Die erzeugten Schlüssel werden im Hauptspeicher des pseudonymisierenden Rechners gehalten, wodurch ein Zugriff auf die Pseudonymisierung nur über die Konfiguration der Pseudonymisierung oder den Hauptspeicher des Rechners erfolgen kann. Beide Angriffsmöglichkeiten stehen nur den Systemadministratoren mit den höchsten Systemrechten zur Verfügung und können nach dem

Handbook of Applied Cryptography, Kapitel 12, Auflage 5, 2001

²⁸ Vgl. Gemell, An Introduction to Threshold Cryptography, In: Cryptobytes Vol. 2, Nr. 3, S. 7, 1997

Stand der Technik nicht verhindert werden. Es handelt sich dabei jedoch i.d.R. um einen sehr kleinen Personenkreis, so dass eine organisatorische Sicherung möglich ist.

3.2 Zwischenergebnis

Die hier vorgestellte Beispielarchitektur unter Verwendung von Pseudonymisierung verwirklicht die gesetzliche Grenzziehung insoweit, als ein umfassendes Screening aller Daten im Klartext technisch nicht und organisatorisch nur unter großen Hürden möglich ist. Eine nachträgliche Umwidmung zu anderen Zwecken wie bspw. der Verhaltens- und Leistungskontrolle könnte höchstens durch das Zusammenwirken der organisatorisch an der Aufdeckung beteiligten Personen und selbst dann nur unter dem erheblichen Mehraufwand der Einzelaufdeckung aller relevanten Pseudonyme geschehen.

Der Betroffene kann sich der Vertraulichkeit seiner Daten sicher sein, solange er sich an die Vorgaben der IT-Sicherheit im Unternehmen hält.

4 Fraud Detection

Maßnahmen, welche auf IT-Ebene zur Betrugserkennung im Unternehmensumfeld getroffen werden, ähneln jenen der Intrusion Detection. Unterschiede ergeben sich daraus, dass Fraud Detection Systeme (FDS) üblicherweise an sogenannte Enterprise-Resource-Planning-Systeme (ERP-System)²⁹ angebunden sind. Ein ERP-System bildet die Standardgeschäftsprozesse aller funktionalen Einheiten des Unternehmens unter Berücksichtigung interner Kontrollen ab, z. B. durch Aufgabenteilung zur Durchsetzung des 4-Augen-Prinzips. Die internen Kontrollen dienen u. a. auch der Vermeidung von Betrug durch die Mitarbeiter des Unternehmens, können diesen aber nicht generell verhindern.

Aufgrund der Verbindung zu externen Akteuren sind Einkauf und Vertrieb neuralgische Punkte für das Auftreten von Betrug durch Mitarbeiter. Dies resultiert einerseits aus den zur Erfüllung der Geschäftstätigkeit notwendigen Spielräumen sowie der Tatsache, dass das Umfeld (externer Akteure) nicht vollständig im ERP-

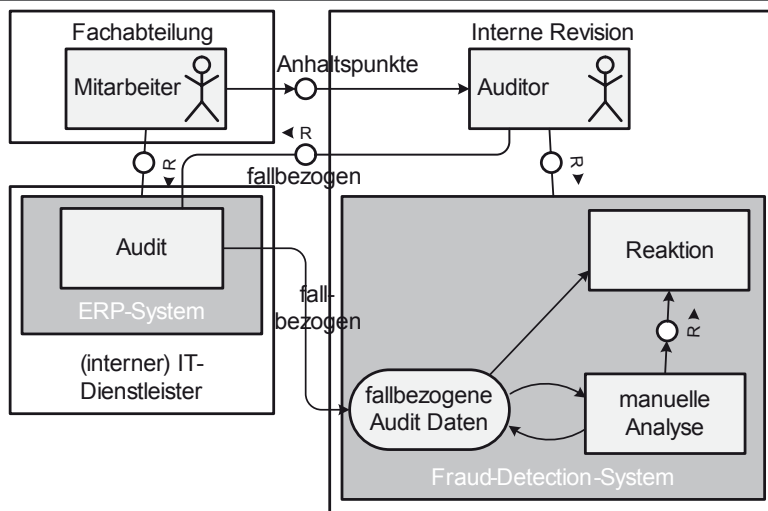
²⁹ Vgl. Gronau, Enterprise Resource Planning und Supply Chain Management: Architektur und Funktionen, 2004.

²⁵ Für die lokale Speicherung der Daten muss das IDS eine Ermittlung der physischen Herkunft wirksam verhindern, so dass darüber keine Zuordnung zu einer Person oder einem Rechner erfolgen kann.

²⁶ Bei symmetrische Verschlüsselungsverfahren kommt bei Chiffrierung und Dechiffrierung derselbe Schlüssel zum Einsatz. Vgl. Menezes/van Oorschot/Vanstone, Handbook of Applied Cryptography, Kapitel 7, Auflage 5, 2001

²⁷ Informationstheoretisch sicher bedeutet in diesem Kontext, dass die sich die Berechnung von k nicht vereinfacht, solange nicht n Schlüsselanteile bekannt sind. Vgl. Menezes/van Oorschot/Vanstone,

Abbildung 3 | Struktur eines Fraud Detection Systems



System abgebildet ist. Es ergeben sich jedoch Anhaltspunkte. So sind bspw. im Einkauf ungewöhnlich häufige und nicht marktbedingte Einkäufer-Lieferant-Kombinationen oder das häufige und möglicherweise gezielte Umgehen kontrollpflichtiger Preisgrenzen als Anhaltspunkte für Betrugsabsichten zu werten.

In gegenwärtigen Systemen stammen Anhaltspunkte regelmäßig nicht aus dem System selbst, sondern von externen Quellen wie bspw. Kollegen und Vorgesetzten. Diese werden von der Revisionsabteilung verfolgt und können zu einer fallbezogenen Datenanalyse führen, wenn diese gerechtfertigt erscheint.

Da die Sichtung des ERP-Datenbestands nur fallbezogen und bei Vorliegen externer Anhaltspunkte stattfindet, ist die Aufklärungsrate tendenziell niedrig. Es stellt sich die Frage, ob die aus diesem Grund vorzugswürdige automatisierte Erkennung von Anhaltspunkten auf ERP-Daten aus gesetzlicher Sicht zulässig ist.

4.1 Aufbau des klassischen FDS

Der Aufbau des betrachteten FDS ist in Abbildung 3 dargestellt. Es besteht im Wesentlichen aus den gleichen Komponenten wie ein IDS mit dem Unterschied, dass sich Audit-Komponente und Audit-Daten nicht auf einem lokalen Arbeitsplatzrechner, sondern auf einem zentralen ERP-Server befinden. Ferner werden die Daten nicht permanent und auch nicht automatisch analysiert, sondern nur manuell bei gegebenem Verdacht.

In diesem Fall fordert der Auditor einen fallbezogenen Auszug aus dem ERP-Da-

tenbestand an. Dieser wird unter Zuhilfenahme manueller Analysewerkzeuge auf weitere Hinweise untersucht. Erhärtet sich der Verdacht gegen den Mitarbeiter, so kann eine entsprechende Reaktion eingeleitet werden.

4.2 Rechtliche Bewertung

Anders als im vorhergehenden Szenario steht hier nicht die Rechtmäßigkeit der Speicherung und Verwendung einer zweckgebundenen Datenbasis im Mittelpunkt. Die Daten des ERP-Systems liegen schon aus Gründen der allgemeinen Geschäftstätigkeit vor. Datenschutzrechtlich relevant ist der Sachverhalt erst dann, wenn auf Grundlage des Anfangsverdachts auf einen Betrugsfall die Daten aus dem ERP-System extrahiert und an das FDS zur Auswertung übertragen werden. Da die Auswertung auf die Ermittlung von Straftaten gerichtet ist, kommt nach der Novelle des BDSG gemäß seinem Wortlaut § 32 Abs. 1 (Alternative zwei) BDSG in Betracht. Da diese Norm jedoch den Anfangsverdacht gerade voraussetzt, stellt er keine Ermächtigungsgrundlage für die automatisierte Ermittlung eben dieses Anfangsverdachts dar.

Um die aus Unternehmenssicht vorzugswürdige automatisierte Erhöhung der Aufklärungsrate zu realisieren, muss deshalb untersucht werden, ob gleichwohl in rechtmäßiger Weise Anhaltspunkte durch die automatisierte Analyse der relevanten Daten im ERP-System gewonnen werden könnten. In systematischer Hinsicht dürfte Alternative zwei in § 32 Abs. 1 BDSG für seinen Anwendungsfall insofern die mit

geringeren Anforderungen versehene Alternative eins des § 32 Abs. 1 BDSG verdrängen.

Da es bei der technischen Gewinnung von Anhaltspunkten für einen Betrugsfall um eine Maßnahme im Bereich der Aufklärung von Straftaten geht, wäre es naheliegend, es hiermit sein Bewenden haben zu lassen. Allerdings gilt es zu beachten, dass die Vorschrift inhaltlich aus der Rechtsprechung des BAG zur verdeckten Videoüberwachung abgeleitet wurde.³⁰ Die besondere Gefährdungslage folgt in diesen Fällen der Videoüberwachung aus dem Umstand, dass alle Mitarbeiter personalisiert einer dauerhaften Überwachung ausgesetzt werden, um zunächst einen Anhaltspunkt für konkrete Maßnahmen zu gewinnen. Ebenso würde es sich auch bei den hier genannten Fällen verhalten, wenn immerwährend Klardaten und Ergebnisse der Auditierung an die interne Revision weitergegeben würden.

Sofern jedoch durch geeignete Maßnahmen der Pseudonymisierung der regelmäßige Personenbezug für die interne Revision entfielen und lediglich im tatsächlichen Verdachtsfall eine Offenlegung erfolgte, könnte die Maßnahme eben nicht in den Anwendungsbereich der speziellen Regelung fallen, sondern in verhältnismäßiger Weise schon durch die erste Alternative des § 32 Abs. 1 BDSG legitimiert werden, welcher mangels Vergleichbarkeit mit den Fällen der zweiten Alternative nicht verdrängt wäre.

5 Pseudonymisierung für FDS

Die Architektur eines Systems zur pseudonymisierten Gewinnung von Anhaltspunkten ist in Abbildung 4 dargestellt. Die Extraktion von Audit-Daten, deren Pseudonymisierung und automatische sowie manuelle Analyse auf Anhaltspunkte tritt in diesem System an die Stelle der Anhaltspunkte durch Mitarbeiter im herkömmlichen Verfahren. Die Anforderungen an die Pseudonymisierung für FDS gleichen jenen, die auch bei IDS formuliert wurden. Zu deren Erfüllung kommen die in den Abschnitten 3.1.1, 3.1.2 und 3.1.3 beschriebenen Verschlüsselungs- und Zerlegungsverfahren zum Einsatz. Die Sicherheit der Zuordnungsregel wird durch eine organisatorische Trennung (vgl. Abschnitt 3.1.4) garantiert. Zusätzlich müs-

30 Erfurt, NJW 2009, 2723

sen die der automatischen Analyse zugrunde liegenden Erkennungsregeln unter Beteiligung von Betriebsrat und Datenschutzbeauftragten so gestaltet werden, dass die hierdurch gefundenen Hinweise den in § 32 Abs. 1 (Alternative zwei) BDSG formulierten Anforderungen an einen Anfangsverdacht genügen. Über diese Regeln wird die *technisch zweckgebundene Zurechenbarkeit* realisiert.

Hinzu tritt, analog zu IDS, die Möglichkeit, dass ein Verhalten zwar auffällig, aber (noch) von keiner Regel abgedeckt ist. Hinweise auf solche Fälle können in der nachgelagerten manuell durchgeführten Analyse auf pseudonymisierten Daten gefunden werden und führen ggf. zu einer Aufdeckung unter Beteiligung der organisatorisch bestimmten Zuständigen. Auf diese Weise wird die *organisatorisch zweckgebundene Zurechenbarkeit* realisiert.

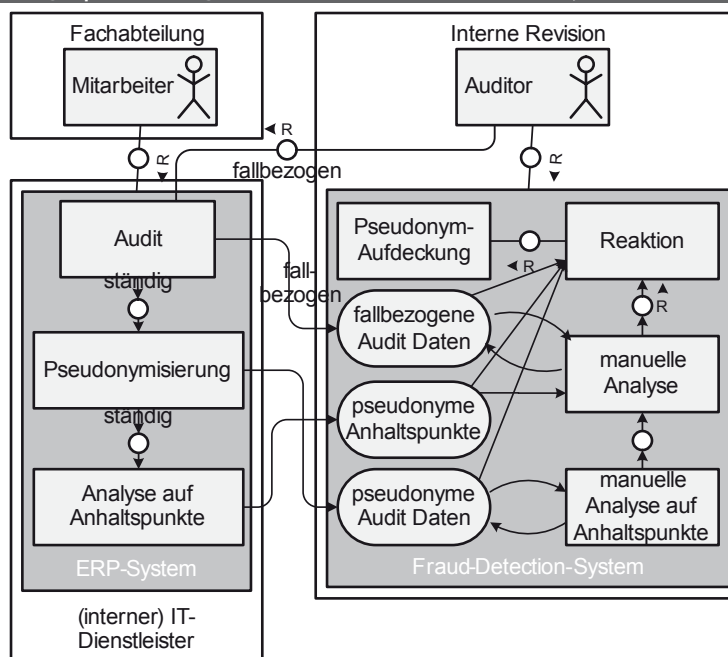
Der Erkennungsvorgang endet, sofern sich ein Anhaltspunkt ergeben hat, mit der *Reaktion der Pseudonymaufdeckung*. Aufgrund des gewonnenen Anfangsverdachts kann der Auditor fallbezogen Klartext-Audit-Daten anfordern, diese manuell analysieren und belastende Information zu Beweis Zwecken sammeln. Hier muss, analog zu dem Verfahren bei herkömmlichen FDS, organisatorisch sichergestellt sein, dass dieser Zugriff erstens nur nach einer Pseudonymaufdeckung erfolgt und zweitens nur solche Daten erfasst, die für diesen Ermittlungsfall notwendig sind, da sich ansonsten das Verbot der umfassenden Analyse auf Klartextdaten umgehen ließe.

6 Fazit

Im Falle der Intrusion Detection stellte sich die Frage, ob eine umfassende Datenerhebung und -analyse sowohl zur Gewährleistung von IT-Sicherheit als auch zur Verhaltens- und Leistungskontrolle zulässig sind. Es wurde herausgearbeitet, dass hinsichtlich des Zwecks der IT-Sicherheit eine solche Zulässigkeit gegeben, das Vorgehen jedoch mit dem Risiko behaftet ist, dass zu diesem Zweck gewonnene Daten ohne Kenntnis des Betroffenen zu anderen Zwecken genutzt werden.

Eine Verwendung zur Verhaltens- und Leistungskontrolle ist hingegen nur mit Beteiligung des Betriebsrats und mit Blick auf das neue IT-Grundrecht nur auf Basis von Stichproben zulässig. Aus daten-

Abbildung 4 | Gewinnung von Anhaltspunkten auf pseudonymisierten Daten



schutzrechtlicher Sicht ist daher zu fordern, dass diese gesetzliche Grenzziehung bei der Gestaltung von hierfür genutzten Systemen von Anfang an berücksichtigt wird. Durch die Pseudonymisierung der Daten nach dem vorgestellten Verfahren wird eine dem Sicherheitszweck entsprechende Nutzung unterstützt, eine nachträgliche zweckabändernde Nutzung der Daten jedoch wirksam verhindert. Aufgrund der gleichen Eignung für den vorgesehenen Zweck und eines verhältnismäßig geringen Mehraufwands kann der Einsatz solcher und gleichwertiger Systeme als rechtlich empfohlen wenn nicht sogar geboten angesehen werden.

Hinsichtlich der Fraud Detection betrifft die Frage die Zulässigkeit einer auf ERP-Daten-Analyse beruhenden Gewinnung von Anfangsverdachten. Im Vergleich zu IDS ergibt sich aus rechtlicher Sicht einerseits der Unterschied, dass hier nicht die Erhebung und Speicherung der Daten im Fokus der Betrachtung steht, da diese aufgrund der Geschäftstätigkeit erhoben werden müssen und auch dürfen, sondern allein die Art der Nutzung. Andererseits handelt es sich im Falle der Betrugserkennung klar um die Aufdeckung und Verfolgung von Straftaten. Hieraus folgend ist mit Blick auf die konkretisierende Normierung des neu eingeführten § 32 BDSG sowie die Literatur und Rechtsprechung zu vergleichbaren Fällen der Telefon- und Videoüberwachung zusam-

menfassend festzuhalten, dass eine Totalkontrolle auf Klartextdaten der gesetzlichen Intention klar widerspricht. Hiernach wäre eine Gewinnung von Anhaltspunkten aus der Datenbasis des ERP-Systems als unzulässig zu werten. Durch die vorgestellte Lösung wird die Analyse auf Klartextdaten durch eine Analyse auf pseudonymisierten Daten ersetzt. Die verwendeten Pseudonyme können nur im konkreten Verdachtsfall aufgedeckt und damit der Personenbezug der Daten wieder hergestellt werden. Dieser Schritt ist aufgrund des zu diesem Zeitpunkt bereits bestehenden Anfangsverdachts zulässig.

Auf diese Weise könnte also die intendierte Erhöhung der Aufklärungsrate von Betrugsfällen bei gleichzeitiger Wahrung der Vertrauenssphäre des Betroffenen erreicht werden. Die Schwäche herkömmlicher FDS, welche auf externe Hinweisgeber angewiesen sind könnte damit also überwunden werden.

Dank

Der Anstoß für diesen Artikel entstand aus einem Inhouse-Projekt der SAP AG. Wir danken insbesondere Herrmann-Josef Schwab, Zoltan Waag und Jürgen Wurth für ihre tatkräftige Unterstützung im Projekt und ihre hilfreichen Anmerkungen zu diesem Artikel.