## 4.5 Zusammenfassung

Nicht mehr nur die produktiven Systeme des Unternehmens bieten Angriffspunkte zur irregulären Nutzung. Die Systemlandschaft wird unübersichtlicher – die Möglichkeit des Datenzugriffs auf Echtdaten ebenso. Es werden immer mehr Systeme mit synchronisierten Zugriffen oder regelmäßig anzustoßenden Extraktionen auf originäre Datenbestände bereitgestellt (BI / BW).

Das datenführende System wird dabei meist in seinen Berechtigungsstrukturen mit an den Fachaufgaben orientierten Rollen beschränkt, aber die Sekundärsysteme häufig durchaus stiefmütterlich behandelt, obwohl auch dort ggf. schreibende Prozesse auf das Primärsystem implementiert werden, zumindest aber (oft in der Felderanzahl beschränkt) die Datenqualität ähnlich hoch oder sogar identisch ist. Entsprechend weit gefasst werden dort teilweise die Berechtigungsstrukturen aufgebaut und den Benutzerstammsätzen zugewiesen. Die Administration der Systeme ebenso wie die privilegierten Stammsätze zur Nutzung von Schnittstellen und Datenkonsolidierungen (z.B. zwischen SAP Classic und HCM) bieten den stärksten Zugriff auf die Systeme. „A key resource in any new SAP implementation or production support organization is the Basis administrator of the SAP system. SAP Basis administration involves all of the system administration activities […].“ [498]

Die Wichtigkeit dieser zentralen Ressource drückt sich – außerhalb jeder Diskussion um notwendige Führungsverantwortung zur Legitimation von Top-Gehältern – häufig denn auch im Stellenwert aus, der auch in der Ausübung der Linienfunktion erheblich sein kann und auch in der Führungsebene so gesehen wird. ”A Basis administrator commands top salaries and a stable job with excellent career progression opportunities in an organization.” [499] Entsprechend der Kurzweiligkeit von Wissen in diesem Umfeld und der hohen Bedeutung einer stetigen, auf hohem Niveau stattfindenden Qualifizierung stellt Mereddy zutreffend fest: “SAP system administration and technical architecture work are challenging and yet provide a rewarding career for an IT professional.”[500]

Welche Motivlage einen Missbrauch von gewährten Rechten in einem IT-System auch immer erklärt und aus Sicht eines Täters vielleicht legitimiert – es ergeben sich nicht nur Risiken in den Primär- und Sekundärsystemen aus der Applikation selbst, der technologischen Basis und den definierten Zugriffsschutzsystemen heraus, sondern auch aus dem Umfang des Nutzerkreises, der Datenextraktion, der Schnittstellenbedienung und der Ablage von Extrakten, der Nutzung dieser und der Aktualität von Daten. Viele sensible Daten – personenbezogen, -beziehbar oder auch wirtschaftlich nutzbar – werden in SAP gehalten und unzureichend vor irregulären Zugriffen

[498] MEREDDY(2011), S. 3.
[499] MEREDDY(2011), S. 3.
[500] MEREDDY(2011), S. 9.

geschützt. Kontoinformationen von Kunden und Beschäftigten bilden nur einen sehr kleinen Bereich hiervon. Wenn aber solche Daten oder Datenextrakte auch mit Aktualitätsversatz vagabundieren und im Schutzbedarf für nicht wesentlich erachtet werden, kann dies zu erheblichen Problemen führen. Gleiches gilt für die Systeme Test, Integration, Qualitätssicherung und ähnlich benannte Systemaufbauten als Produktionskopie als Ansatzpunkte zur missbräuchlichen Nutzung. [501]

Aus Sicht der Wirtschaftsinformatik sind die unternehmensindividuellen Topologie- und Konfigurationsrisiken eingrenzbar und bei Verantwortlichen der IT-Dienstleister bekannt. Obwohl die überwiegenden Protokollierungen grundsätzlich unzureichend sind und im Spannungsfeld zwischen einer hohen Aussagekraftforderung und einer Volumenerzeugungs- und Nachvollzugszeitproblematik stehen, führt dies zu einer insgesamt eher geringen Risikoeinschätzung. Problematisch sind die Risiken, die sich aus dem Einspielen und Entwickeln von Software / Quellcode ergeben. Sowohl SAP selbst als auch SAP-funktionale Integrationsdienstleister stellen regelmäßig Code zur Verfügung, der durch das einsetzende Unternehmen nicht in seinem Wirkungsrisiko betrachtet werden kann. Sicherheitshinweise durch SAP selbst und SAP Security Researcher werden zwar (vorausgesetzt, sie werden durch SAP als solche anerkannt) durch Patches beseitigt, aber zwischen Bekanntwerden relevanter Sicherheitslücken, die durch externe Researcher gefunden wurden, und dem jeweils zugehörigen Patch (ob explizites Patch, Multi-Patch für mehrere Lücken oder Silent Patch) können zwischen einem Monat und mehrere Jahre vergehen (Beispiel Transaktion SAT und SE30 von Seite 132ff. insgesamt etwa zwei Jahre nach Bekanntwerden, letzter SAP-Hinweis aus 2012). Es gibt Aussagen, dass zwei Schwachstellen pro Woche durch externe Security Researcher entdeckt werden. Ob dies nachvollziehbar ermittelt wurde, ist nicht bekannt. Aber die Diskrepanz zwischen Erkennen und Schließen von Sicherheitslücken öffnet Angreifern Möglichkeiten, Angriffs-Szenarien zu testen und umfassend zu platzieren. Ein aktives Patch-Management, also das zeitnahe Einspielen von Patches ohne Security Gap im Unternehmen, wiegt zunächst in Sicherheit. Trotzdem entsteht ein viel zu großes zeitliches Fenster für Angriffe, sei es von innen oder von außerhalb des Unternehmens. Auch bei selbsterstelltem Quellcode ist die Gefahr des Innentäterangriffs grundsätzlich hoch und im Schadenfall kaum nachvollziehbar. Im aufgetretenen Beispiel auf Seite 131 zeigt sich das Dilemma. Ein Quellcode muss nicht von sich aus schädlich sein, vielmehr öffnet er das System für den Import beliebigen Codes und lässt im Nutzungsfall wie beschrieben verantwortlich Handelnde im Unklaren. Ein Nachvollzug ist nicht möglich. Ferner ist feststellbar, dass Schnittstellenüberwachungen und die Rechte hoch privilegierte Benutzer (intern / extern) auch weiterhin problematisch bleiben. Eine wirkungsvolle Eingrenzung und Überwachung von mit umfassenden Rechten versorgten Beratungs-, Administrations-, Modulbetreuungs-, System- und Schnittstellen-Accounts ist kaum realisierbar, es sei denn, es gelingt in der Zukunft, die Administration des Systems und die Kommunikation zwischen Systemen von den Zugriffsmöglichkeiten auf die Business-Daten zu entkoppeln.

[501] Vgl. TIEDE(2004), S. 596f.

## 5. Schlussfolgerungen

Der Gesetzgeber hat in der Vergangenheit trotz zunehmender Regulation [502] auch aus handels- und datenschutzrechtlicher Sicht, hinsichtlich Kontrolle und Transparenz im Unternehmensbereich und sogar aus formulierten Mindestanforderungen an das Risikomanagement kaum konkrete Vorgaben zur IT-Risikobetrachtung gemacht – weder zur IT als Risikofeld noch zur IT als Risikobewältiger. [503] „Alle gesetzlichen Vorgaben umfassen im Kern die folgenden vier zentralen Anforderungen:

- Die wesentlichen Risiken des Unternehmens sind systematisch zu identifizieren.
- Die identifizierten Risiken müssen quantifiziert und in verständlicher Form an die Geschäftsleitung berichtet werden.
- Es sind geeignete Maßnahmen zur Begrenzung und Steuerung der Risiken zu ergreifen.
- Es muss ein internes Kontrollsystem aufgebaut werden, um Risiken zu vermeiden.“ [504]

In welcher Granularität, also mit welchem Tiefgang / welcher Intensität oder auch Aggregation dies erfolgt, wird nicht festgelegt und liegt im Gestaltungsspielraum des Unternehmens, nur Formalismen zu erfüllen, oder aber aussagekräftige Steuerungsmechanismen zu integrieren. Insoweit darf es Aktivitäten im Bereich der IT-Sicherheit, des Berechtigungsmanagements und auch des Datenschutzes bei Bedarf auf ein argumentativ vertretbares Minimum herunterschrauben. Dies mag auf den ersten Blick nicht klug erscheinen, allerdings ist es ein Trugschluss anzunehmen, Entscheidungen des Managements werden immer rational und ohne Zielkonflikt gefällt. In Zeiten zunehmenden Drucks auf die finanzielle und personelle Ressourcenbereitstellung sinken die Spielräume des unternehmerischen Handelns. Sinkende Vertriebsmargen, „eine kontrovers diskutierte Förderung und Vorrangbehandlung im Netz von erneuerbaren Energien, eine Belastungsreduzierung energieintensiver Industrieunternehmen zulasten der Privathaushalte und KMU, die Anreizregulierung mit sinkenden Netzentgelten und die gleichzeitige Debatte um den Netzausbau bei fraglicher Investitionsrendite“ [505], aber auch die derzeit problematische Vermarktung der eigenen Erzeugung speziell bei historisch bedingter, auf Basis fossiler Energieträger stattfindender Produktion (hohe Bereitstellungs- und Produktionskosten bei geringen Vermarktungserlösen) führt eher zu Kompensationsbemühungen durch Erschließen neuer Geschäftsfelder – z.B. durch Gesellschaftsbeteiligung in der Biogaserzeugung oder Contracting – und erzeugungs- und vertriebsoptimierender Prozessunterstützung. Dies sind die Bereiche, in die die finanziellen Mittel fließen. Die höchste Priorität erhalten Themen wie IT-Sicherheit, Daten- und Systemzugriffsschutz in solchen Zeiten nicht. Aus Unternehmersicht gibt es also ebenso viele Gründe, den betrieblichen Datenschutz, die IT-Sicherheit und die IT-Revision in seinen Möglichkeiten der Analyse, konstruktiven Kritik und Teilhabe an Entscheidungen zu begrenzen

[502] Vgl. ERWIN/MARLINGHAUS(2013), S. 20f., hinsichtlich eines Continuous Monitoring zur Risikosicht.
[503] Vgl. KAPFFER/KAUFER(2013), S. 12.
[504] KAPFFER/KAUFER(2013), S. 12f.
[505] WILDENSEE(2013), S. 187.

wie es Gründe gibt, Administratoren und privilegierte Systembetreuer in ihren Systemrechten zu beschneiden. Es ist zunächst auch immer eine Diskussion der Kosten-Nutzen-Relation. Es kann darüber hinaus festgestellt werden, dass rechtliche Rahmengebungen fehlen, um ein Unternehmen bzw. verantwortlich handelnde Personen zu mehr als dem Minimum im Bereich der IT-Sicherheit und IT-Revision, des Berechtigungsmanagements und auch des Datenschutzes zu zwingen und im Bedarfsfall wirkungsvolle Sanktionen zu verhängen. Der Gesetzgeber – sowohl der nationale als auch der europäische – war bisher kaum gewillt oder über die Konsensverwerfungen der EU in der Lage, mehr als die bisher häufig unpräzise formulierten Inhalte zu fordern und Unternehmen Pflichten aufzutragen mit kausal eindeutiger Ursache-Wirkungslinie (d.h. „bei Verstoß erfolgt eine Strafe“). Wenige, rechtlich eindeutige Vorgaben müssen natürlich Beachtung finden, insbesondere aus dem Handels- und Datenschutzrecht. Das definierte Minimum mit geringer Nachweisführung läuft immer Gefahr, im Schaden- bzw. Prüfungsfall nicht auszureichen und zu einem sanktionsfähigen Tatbestand zu werden. Wie dargelegt reicht die partielle Orientierung an vorhandenen Standards und Leitfäden aber häufig aus, um Tätigkeit belegen zu können. Beachtenswert ist im Schadenfall, dass der durch stark berechtigte Systemnutzer eigenmotivierte Missbrauch von Zugriffsberechtigungen allgemein juristisch und speziell arbeitsrechtlich keine Herausforderung bei der Schuldfeststellung darstellt, wenn der Nachweis geführt werden kann. Der durch Vorgesetzte initiierte Missbrauch solcher Zugriffe durch rechteprivilegierte Beschäftigte ist allerdings besonders perfide, bedeutet er doch das Ausnutzen der aufgaben- bzw. rollenbezogenen Anweisungsbefugnis des hierarchisch höher gestellten Vorgesetzten. Funktionsnutzungen, protokolliert in den Details der IT-Systeme und als Verfehlungen identifiziert, sind unproblematischer zu belegen, als ausschließlich artikulierte, nachweislose Anweisungen der höheren Hierarchie, wenn fehlende (Un)Rechtskenntnis Handelnder bei einem Verstoß gegen Regularien vorliegt.

Ein vollumfängliches Vernachlässigen vorhandener Standards, so z.B. die Hinweise und Leitfäden der Solution-Hersteller und der weithin anerkannten DSAG, wäre insbesondere für verantwortlich handelnde Personen der IT und des Top-Managements sträflich, denn gerade diese Vorgaben gelten als „best practice“ und können insoweit kaum ignoriert werden. Allerdings reichen an den Zielen des Unternehmens ausgerichtete Teilumsetzungen aus, wenn das Unternehmen über Security- und Data Privacy-Policies den Willen hierzu dokumentiert (insoweit vieles nur im Soll und weniger im Ist). Die IT-Sicherheit und der betriebliche Datenschutz dürfen durchaus „an die Kandare“ genommen werden. Die IT-verantwortlichen Bereiche werden dabei auch immer für Teilumsetzungen sorgen, denn ausgesuchte Punkte der Themen IT-Sicherheit und Datenschutz der Leitfäden finden sich bereits in den technischen Implementationsleitfäden der eingesetzten Produkte.

Für den Bereich der Berechtigungsherstellung und rollenbasierten Zuweisung in SAP führt dies zur Darlegung, dass bis auf wenige Ausnahmen – z.B. aus der Datenzugriffstrennungsnotwendigkeit von Netz und Vertrieb über das Energiewirtschaftsgesetz – zunächst kaum verpflichtend konkrete Vorgaben existieren, welche Rollen, Zugriffsdefinitionen, Detailberechtigungen und Funktionstrennungen im Unternehmen vorhanden sein müssen oder nicht sein dürfen. Wirtschaftliche Zwänge, z.B. die aus Branchen-Benchmarks abgeleitete Reduzierungsnotwendigkeit von Personal- und Prozesskosten, können immer als Begründung herhalten, um weitreichende Berechtigungen in wenigen Rollen zu bündeln und diese zu verteilen oder auch anerkannt notwendige Funktionstrennungen unberücksichtigt zu lassen und somit ein „Need-to-Know"-Prinzip teilweise zu unterlaufen. Konkrete Vorgaben für den Bereich der IT-Sicherheit wurden lediglich dort gefasst, wo eingesetzte Technik aus elementaren Sicherheitsaspekten heraus zu reglementieren ist, z.B. im Bereich der Netzleittechnik. In § 11 Abs. 1a EnWG wurde festgelegt, dass Netzbetreiber einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme sicherzustellen haben, die der Netzsteuerung dienen. Dort heißt es: „*Der Betrieb eines sicheren Energieversorgungsnetzes umfasst insbesondere auch einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die der Netzsteuerung dienen. Die Regulierungsbehörde erstellt hierzu im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen Katalog von Sicherheitsanforderungen und veröffentlicht diesen. Ein angemessener Schutz des Betriebs eines Energieversorgungsnetzes wird vermutet, wenn dieser Katalog der Sicherheitsanforderungen eingehalten und dies vom Betreiber dokumentiert worden ist. Die Einhaltung kann von der Regulierungsbehörde überprüft werden.* […]" Hier wird folglich im Zusammenspiel zwischen Bundesnetzagentur und dem BSI eine verpflichtend anzuwendende Grundlage geschaffen. Es folgt ein Verweis auf einen derzeit im Entwurf vorhandenen Sicherheitskatalog der Bundesnetzagentur. In diesem werden z.B. die Einführung eines Informationssicherheitsmanagementsystems (ISMS) sowie die Benennung eines IT-Sicherheitsbeauftragten gefordert. Dies betrifft allerdings ausdrücklich IT-Systeme, die die Netzsteuerung ermöglichen und unterstützen. Diese wiederum gelten nicht als rechnungslegungsrelevant, da hier keine Daten generiert, umgewandelt oder aufbereitet werden, die in der Rechnungslegung oder einem Vor- oder Nebensystem Verwendung finden. Jedoch ist erkennbar, dass auf einem solchen Wege durchaus Ansprüche in Unternehmen transportiert werden können und die Umsetzung in einen Überprüfungs- und ggf. sogar Anordnungs- und Sanktionsweg münden.

Prüfinstanzen wie die Landesdatenschutzbehörden werden üblicherweise nur auf Veranlassung tätig, d.h. wenn Betroffene eine (zumeist anonyme) Beschwerde verfassen und die Aufsichtsbehörde dieser dann punktuell nachgeht. Im Fokus sind dabei das entsprechend monierte Verfahren, bei dem personenbezogene oder -beziehbare Daten verarbeitet werden, und die Dokumentation nach weitgehend formellen Vorgaben des BDSG. Das Berechtigungskonzept selbst ist (trotz § 9 BDSG,

Anlage zu § 9 und i.V.m. § 3a BDSG [506]) kaum in der Sicht, denn hierfür müsste – schon aufgrund des nicht selten erheblich dokumentarischen Umfanges – Prüferkapazität und spezifisches Know-how vorhanden sein, um Fehler oder bewusste Täuschungen und Zielkonflikte erkennen zu können. Dies ist kaum zu gewährleisten. Und die Funktion des betrieblichen Datenschutzbeauftragten als Teil der betrieblichen Selbstkontrolle läuft trotz eines häufig adäquaten Know-how-Vorsprungs Gefahr, im Fall von Interpretationskontroversen mit dem Arbeitgeber gegen arbeitsvertragliche Treuepflichten zu verstoßen, wenn er zur Klärung eigenmächtig die zuständige Prüfinstanz einbezieht und auf die Misere explizit hinweist. Er kann sich dauerhaft selbst beschädigen.

Insoweit verharrt die Durchsetzungskraft der prüfenden Datenschutzaufsichtsbehörden und auch des betrieblichen Datenschutzbeauftragten bei der betrachteten Thematik häufig im erreichten Status Quo weitgehender Mittelmäßigkeit. Obwohl sowohl allgemein gesetzliche als auch konkreter auf freiwilliger Basis anzuwendende Vorgaben zur proaktiven Identifizierung und Bewältigung von Risiken – speziell auch für das IT-Umfeld – in Unternehmen existieren, kann keine Aussage über die Gewährleistung der inhaltlichen Korrektheit, Formulierungsneutralität, Vollständigkeit und Wirksamkeit definierter Kontrollmaßnahmen in den Unternehmen getroffen werden. Dies gilt für die Anwendung aller Vorgehensmodelle zur Risikobetrachtung und zum (IT-)Risikomanagement – im geführten Diskurs z.B. auch für Common Criteria (als Standard nachrangig und daher unbetrachtet, da als strukturgebende Vorgabe inhaltlich regelnd ohne wesentliche Differenz zu HGB, AO und FAIT [Authentifizierung, Logging, aufgaben- und rollenbasiertes IAM etc.] und nicht konkreter in der Vorgabenentwicklung zur Basisabsicherung und Rollenausgestaltung in SAP-Systemen).

Einzig der Wirtschafts- / Abschlussprüfer kann aufgrund seiner legitimierten Aufgabenwahrnehmung für Abhilfe sorgen. Dieser weist im Rahmen des erteilten Mandats und der jahresabschlussnahen Prüfung zumeist sowohl die Kapazität als auch das Wissen auf, um kritisch prüfend im Detail zu hinterfragen. Ob diese Inhalte Prüfungsinhalt sind, ist auftragsbezogen und nicht immer gegeben. In der Abstimmung des Mandats werden aber häufig bereits Vorschläge unterbreitet, die auch die Berücksichtigung des Berechtigungskonzeptes mit spezifischem Prüfungsfokus einschließen. Wenn die Begutachtung auch dieser Inhalte durchgeführt werden soll, ist neben der rein zeitlichen Dimension auch die Know-how-Abdeckung zumeist auf hohem Niveau gegeben. Dafür sorgen der Umfang vorhandener Prüferkapazitäten, der Informationsaustausch der Prüfungsteams untereinander und der punktuelle Einbezug spezialisierter Prüfer/-innen in die Auftragsabwicklung. Diese orientieren sich an den Vorgaben der IDW-Standards und der anerkannt umfangreichen Literatur zum Produkt / Verfahren (DSAG, Leitfäden der Hersteller, Fachliteratur, auch der speziellen Revisionsliteratur). Sicherlich bedeutet dies nicht, dass Forderungen in den höchsten Ausprägungen herausgestellt werden.

[506] Die Orientierung des IT-Einsatzes an dem Grundsatz der Datenvermeidung und Datensparsamkeit findet kaum Anklang in den Unternehmen und wird auch von den Aufsichtsbehörden als untergeordneter Aspekt angesehen. Vgl. SCHOLZ, in: SIMITIS(2011), BDSG, § 3a, Rn. 6.

Ein gewisses Maß an Interpretierbarkeit und ein notwendiges Eingehen auf unternehmensindividuelle Belange führen zu einem Ermessensspielraum in Detailfragen. Aber es werden zumindest weitgehende Teilumsetzungen gefordert.

Dies führt im Rahmen der Diskussion um eine rollenbasierte Berechtigungsherstellung mit auszuprägenden Rollen und Berechtigungen und einer aufgabenbezogenen Zuweisung zu verantwortlichen Personen(gruppen) und dabei als notwendig erkannten Funktionstrennungen letztlich zur abschließenden Sicht auf den Rechtsrahmen deutscher Unternehmen:

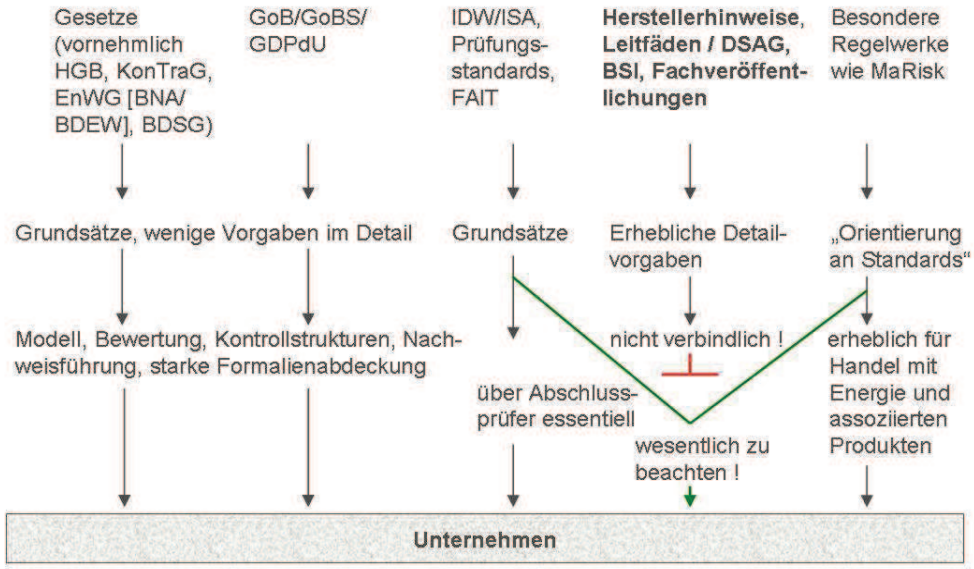


Abb. 5-1: Wesentliche Einflüsse auf die Ausgestaltung von SAP-Berechtigungskonzeptionen in Unternehmen (Eigene Darstellung). [507]

Für Unternehmen ist die Sicht auf die wesentlichen Einflussgrößen sehr wichtig, erlaubt sie doch eine Abstufungseinschätzung der Wesentlichkeit regulatorischer Vorgaben auch unter wirtschaftlichen Abwägungen. Insbesondere der nicht-gesetzliche Regulationsrahmen führt zu einem nicht zu unterschätzenden Umsetzungsdruck in den Unternehmen. Es ist darüber hinaus ebenfalls sinnvoll, wenn die Spezialisierungen in der Internen Revision – zu sehen als Elemente der betrieblichen Selbstkontrolle trotz differierender Legitimation und inhaltlicher Fokussierung gegenüber dem betrieblichen Datenschutz und der IT-Sicherheit mindestens in den Fragestellungen des IAM, der Systembasissicherheit und zu ihren spezifischen Bearbeitungsaspekten als Verbündete im Geiste – die Maßstäbe aus den Prüfungsstandards des IDW annehmen, ihre Prüfungen als abschlussnahe Prüfungen simulieren und ebenso die Beratungen und Begutachtungen danach ausrichten. Eine Diskussionsgrundlage ist gegeben.

[507] Vgl. auch THELEMANN(2010), S. 9f (aus der Berechtigungsstrukturdiskussion heraus mit Vereinfachung).

„Zwischen dem Prüfungsausschuss des Unternehmens, dem externen, d. h. dem gesetzlichen Abschlussprüfer und dem internen Prüfer sollte ein regelmäßiger Dialog gewährleistet sein. Dies würde sicherstellen, dass es keine Lücken bei Compliance und Risikoüberwachung sowie der substanziellen Überprüfung von Vermögenswerten, Verbindlichkeiten, Erlösen und Aufwendungen gibt.“ [508] Dies bedeutet, dass bei Prüfungen im Bereich der rechnungslegungsrelevanten Systeme immer die Fragen aufgeworfen werden: Wie würde ein Abschlussprüfer vorgehen ? Welche inhaltlichen Schwerpunkte würde er setzen ? Der Abschlussprüfer ist gehalten, die Prüfberichte der Internen Revision aus der vorangegangenen Periode einzusehen, um sich einerseits von den Schwerpunkten, vom Tiefgang und der Qualität der Arbeit zu überzeugen (Betrachtung hinsichtlich der Wirksamkeit der Internen Revision), und andererseits abzuleiten, ob hieraus Schwerpunkte auch für ihn ableitbar sind. So kann durch Vorwegnahme eines zielgerichteten Prüfungsvorgehens die Interne Revision für das Unternehmen eine schützende Rolle einnehmen und, zumindest beeinflussend auf die Zielsetzungen der abschlussnahen Prüfungen, einen dezidierten Wertbeitrag leisten – ein Schutzmechanismus vor den Gefahren, die eine gesetzlich legitimierte Prüfinstanz mit impliziter Möglichkeit der Auslösung von Negativeffekten für das Unternehmen mit hohem Maß an Ermessensspielraum bedeutet.

Es bleibt anzumerken, dass die detaillierten Hinweise der Hersteller, der umfangreichen Leitfäden und der Fachliteratur zu Aspekten des Berechtigungswesens, d.h. der Festlegung von abgestuften Rollen, aufgabenorientierten Berechtigungsdefinitionen und ausschließenden Funktionstrennungen und Objektsteuerungsfeldausprägungen, **möglicherweise keine so große Relevanz** hätten, wenn nicht die jährlich wiederkehrende Funktion des gesetzlich legitimierten Abschlussprüfers die Testierung des Jahresabschlusses flankieren würde mit Risikobetrachtungen des IT-Umfeldes, denn diese Aufgabe fällt ebenfalls dem Abschlussprüfer zu. „Im Rahmen der Jahresabschlussprüfung hat der Abschlussprüfer zu beurteilen, ob die auf IT-Systemen gestützte Rechnungslegung den gesetzlichen Anforderungen entspricht, um auf dieser Basis dann eine Prüfungsaussage über die Ordnungsmäßigkeit der Buchführung zu machen. Die gesetzlichen Anforderungen richten sich insbesondere an die Sicherheit und die Ordnungsmäßigkeit der für die Rechnungslegung eingesetzten IT-Systeme und ihres Betriebs.“ [509] Er muss sich also – und dies zeigt die starke Abhängigkeit vom Kompetenzaufbau des im Unternehmen eingesetzten Wirtschaftsprüfers – u.a. davon überzeugen, dass ein funktionsfähiges Risikomanagementsystem implementiert wurde, das auch inhärente IT-Risiken betrachtet. Die konsequente Betrachtung des jeweils umgesetzten Berechtigungskonzeptes in den rechnungslegungsrelevanten IT-Systemen kann dabei eine fruchtbare Aufgabe sein.

[508] GRÜNBUCH(2010), S. 9.
[509] RÜTER/SCHRÖDER/GÖLDNER/NIEBUHR(2010), S. 213.

In der vorliegenden Diskussion beinhalten modul- und funktionsbezogene Zertifizierungen bzw. Aussagen zur Gesetzeskonformität von Softwareprodukten und -funktionalitäten durch Wirtschafts- / Abschlussprüfer oder andere Zertifizierungsunternehmen wenig Mehrwert, wenn es um die Frage des konformen Einsatzes der Eigenentwicklung und der Installationsspezifika geht, denn sie referenzieren ausdrücklich auf Module und Funktionen im beschriebenen Herstellerstandard. Während der Installation und nachfolgend wird jedoch kundenspezifisch angepasst. Dieses Customizing findet keinen Eingang in derartige Einlassungen der Wirtschaftsprüfer oder sonstiger Anbieter.

Es wäre folglich angebracht, dass vor dem Hintergrund einer durch die Steuerpflichtigen zu gewährleistenden Gesetzeskonformität rechnungslegungsrelevanter IT-Systeme letztlich federführend insbesondere das Bundesministerium der Finanzen die Risiken sieht, die auf SAP-Installationen durch die genutzten Technologien und Bereitstellungsvarianten wirken, diese nicht als regulativ zu vernachlässigen darlegt und erkennt, dass es die konkreten Gegenmaßnahmen, die als maßgebliche „best practice“ – vornehmlich zu Risiken „außerhalb des Standards“ – formuliert vorliegen, zumindest für Produktivsysteme als verbindlich ansehen sollte, z.B. mindestens alle Herstellerhinweise (Notes) mit Bezug zu sicherheitskritischen Berechtigungsobjekten und Steuerungsfeldausprägungen, administrativen Funktionen und privilegierten Nutzerrechten. Die Risiken und Lösungsansätze sind technisch anspruchsvoll und kaum generisch formulierbar, aber dennoch könnte die Erwartung im Sinne detailliert produktspezifischer Bestimmungen formuliert werden, dass die Steuerpflichtigen diese Maßnahmen umzusetzen und auch die Wirtschafts- / Abschlussprüfer die Umsetzung derart zu prüfen haben. Dies würde zwar als ein Beschneiden der organisatorischen Gestaltungsfreiheit in den Unternehmen wahrgenommen werden, trüge allerdings die Chance in sich, die Gestaltung und auch Prüfung effizienter vornehmen zu können und weniger Ausnahmen in der Detailgestaltung zuzulassen. Ferner könnten auch Grundsätze formuliert werden, die für alle Softwareanbieter gelten, so z.B. zur Funktionsbereitstellung zum Umgang mit Datenmanipulationen direkt in der Datenbank und der Gewährleistung aussagekräftiger Protokollierungen, Auswertungsmöglichkeiten und Speicherfristen und Volumina von Protokolldateien.

Es besteht gleichsam die Möglichkeit, die Umsetzung der BSI-Maßnahmenkataloge, die auf die herstellerspezifischen Security-Dokumentationen und anerkannten Literaturbesprechungen entsprechender Themen verweisen, trotz Aktualitätsversatzes in den Maßnahmendefinitionen einzufordern. Sinnvoll kann es dabei sein, die BSI-Maßnahmendefinitionen mit SAP Hinweisen der letzten Jahre berechtigungsobjektbezogen zusammengehörig zu gruppieren.

| Objekt | BSI-Referenz | Seite im Maßnahmenkatalog (Seite in BSI(2013)) | Kurzbeschreibung | SAP Note |
|---|---|---|---|---|
| S_DEVELOP | G2.108 | S. 131 (559) | Unterlaufen von Sicherheitsmechanismen, wenn S_DEVELOP mit ACTVT 01 oder 02 in Produktionssystemen zu finden ist | 1420281 (Abschalten von &SAP_EDIT),<br>1465138 (Transaktion SAT mit Tips & Tricks per SQL-Statement ohne Protokollierung über Hack-Tool, abgestellt durch Patch, aber relevant durch nicht immer aktuell gehaltene Systemstände in den Unternehmen),<br>1661349 (Rechteausweitung möglich durch Transaktion SE30 und Tips&Tricks),<br>1263939 (Trace mit SYST in Verbindung mit ACTVT 01 als separierte Berechtigung einzupflegen). |
| S_DEVELOP | M2.349 | S. 794 (2084) | Analog | |
| S_DEVELOP | M4.261 | S. 519 (3275) | Die Profile SAP_ALL, SAP_NEW* und S_DEVELOP* dürfen in einem Produktionssystem nicht genutzt werden, SAP_ALL mit Referenz auf M2.347, S. 789 (2079) | |
| S_RFC | M2.347 | S. 791 (2081) | S_RFC als kritisches Autorisierungsobjekt | 1682316 (RFC-Berechtigungsreduzierung bei Schnittstellen- und sonst privilegierten Usern bei Notwendigkeit des Zugriffs per RFC)<br>1980618 (In RS_FUNCTIONMODULE_INSERT ist die Berechtigungsprüfung nur für externe Aufrufe über RFC obligatorisch; auch Sicherheitshinweis 1589919 und SAP-Note 1826448),<br>1965180 (Unterschiedliche Strenge in der RFC-Authority-Überprüfung),<br>1664340 (Missverständliche Dokumentation bei RFC_TYPE und RFC_NAME bei der Frage, wie der Baustein geschützt wird) |
| S_RFC | M4.263 | S. 523f. (3279f.) | Analog | |
| S_RFC | M5.126 | S. 274f. (4034f.) | Analog, auch Absicherung über SNC | |

| Objekt | BSI-Referenz | Seite im Maßnahmenkatalog (Seite in BSI(2013)) | Kurzbeschreibung | SAP Note |
|---|---|---|---|---|
| S_TABU_DIS | M2.347 | S. 791 (2081) | S_TABU_DIS als kritisches Autorisierungsobjekt | 1481950 (S_TABU_NAM zur expliziten Zuweisung von Tabellen für den Zugriff trotz restriktivem Zugriff auf Tabellengruppen),<br><br>1516880 (Berechtigungsgruppen, auch &NC&, werden nicht weit verteilt, Zugriff über S_TABU_NAM soll stattfinden, Transaktion SE16 unterstützt nicht *NAM). |
| S_TABU_DIS | M4.264 | S. 526f. (3282f.) | S_TABU-Objekte zur Steuerung von Tabellenzugriffen | |
| S_RZL_ADM | M4.258 | S. 508 (3264) | Restriktive Vergabe der Berechtigung, externe Betriebssystemkommandos auszuführen oder zu pflegen. | 1520462 (Unautorisierter Aufruf durch Angreifer von Betriebssystemkommandos mit Parameterstring, da die Funktion keine Berechtigungsprüfung beinhaltet. Prüfung auf S_RZL_ADM mit ACTVT 01),<br><br>1917381 (Nutzen der Profilpflege, obwohl der Zugriff beschränkt sein sollte. In der Profilpflege fehlen Berechtigungsprüfungen für den Zugriff auf bestimmte Funktionen. S_RZL_ADM mit ACTVT 01 wird nun geprüft.),<br><br>1614259 (Kommunikationskanal; Ausführung beliebiger Betriebssystemkommandos, schädlicher Code wurde in MII12.1 SP06 und MII12.2 SP 02 entfernt). |
| […] | | | | |

Tab. 5-1: Exemplarisches Matchen von BSI-Maßnahmenkatalogeinträgen zu SAP-Notes zu bestimmten Berechtigungsobjekten. (unbetrachtet: SAP-Notes-Meldungsjahr, System-/Modulbezug, Korrekturart [Patch, Rollenanpassungen etc.] usw.)

Ebenfalls wäre es auf der Ebene der Wirtschafts- / Abschlussprüfer möglich, gravierende Verfehlungen abgestuft verpflichtend mit Testatformulierungen zu allokieren, um eine bewusste Außenwirkung zu erzielen.

Die Varianten würden vorhandene und auch zukünftige Lösungen zum Standard erklären, Unternehmen zur Umsetzung eines hohen Maßes an „Awareness" – auch in den Führungsebenen – und einer Positionierung auf Linie zwingen sowie die Prüfinstanzen stärken, wenn diese auch zu notwendigen Rollenwahrnehmungen, -definitionen und Funktionstrennungen üblicherweise keine Aussagen zulassen und somit nach wie vor genügend Gestaltungsfreiheit in Unternehmen verbleibt.

Die Kritik an der Arbeit der Wirtschaftsprüfer – speziell in Bezug zur Finanzbranche und in der Verbindung von Jahresabschlussarbeiten und Beratertätigkeit – ist bekannt und nachvollziehbar. „Um ihrer besonderen Verantwortung für Markt und Gesellschaft Rechnung zu tragen, ist vollständige Unabhängigkeit die erste Berufspflicht von Wirtschaftsprüferinnen und Wirtschaftsprüfern und wurde als solche in der Wirtschaftsprüferordnung gesetzlich festgeschrieben (§ 43 Abs. 1 WPO). Steht die Unabhängigkeit in Frage, kann ein Wirtschaftsprüfer sein Mandat per Definition nicht mehr erfüllen. Deshalb sehen wir es als problematisch an, dass Wirtschaftsprüfung und andere (oft hochbezahlte) Beratungsleistungen von den gleichen Firmen durchgeführt werden. In dieser Konstellation testieren Prüfer letztlich Finanzprodukte und Bilanzierungsentscheidungen, die sie selbst – wenn auch in anderen Unternehmensteilen – in ihrer Eigenschaft als Berater entwickeln und unterstützen. Damit sind Interessenskonflikte unausweichlich." [510] Dies kann allerdings kaum als Begründung ausreichen und ist – basierend allein auf der Erfahrung mit der Finanzbranche in den letzten Jahren – auch viel zu plakativ, die abschlussnahen IT-Systemprüfungen der Wirtschaftsprüfungsgesellschaften mit Fokus auf den implementierten Funktionstrennungen / „SoD" und dem Ausschluss systemkritischer Zugriffsrechte in rechnungslegungsrelevanten Systemen einzuschränken. Gesetzlich einengende Regelungen hat es entsprechend bisher nicht gegeben. Eine gesetzliche Regulation dieses Aspekts tilgt ggf. auch die positiven Aspekte und Erfahrungen aus anderen Branchen wie der Energiewirtschaft.

Die vorliegende Arbeit zeigt, dass eine rollenbasierte Berechtigungskonzeption mit implementierten Funktionstrennungen praktikabel ist. Hinzukommen muss eine analoge Diskussion auch für die Betriebssystem-, Netzwerk- (bei contentabhängiger Kommunikationsverschlüsselungsnotwendigkeit), Portal- und Datenbanksicherheit [511], um die Betrachtung der Sicherheitsebenen – unter Einbezug der weiteren Systemstufen (Entwicklung / Test / Integration / Qualitätssicherung) und der Abgrenzung insbesondere unterschiedlicher administrativer und sonst privilegierter Aufgabenwahrnehmungen [512] – für die relevanten SAP-Systeme zu komplettieren.

---

[510] GRUENE(2012), S. 4.
[511] Vgl. RÜTER/SCHRÖDER/GÖLDNER/NIEBUHR(2010), S. 202.
[512] Vgl. RÜTER/SCHRÖDER/GÖLDNER/NIEBUHR(2010), S. 244.