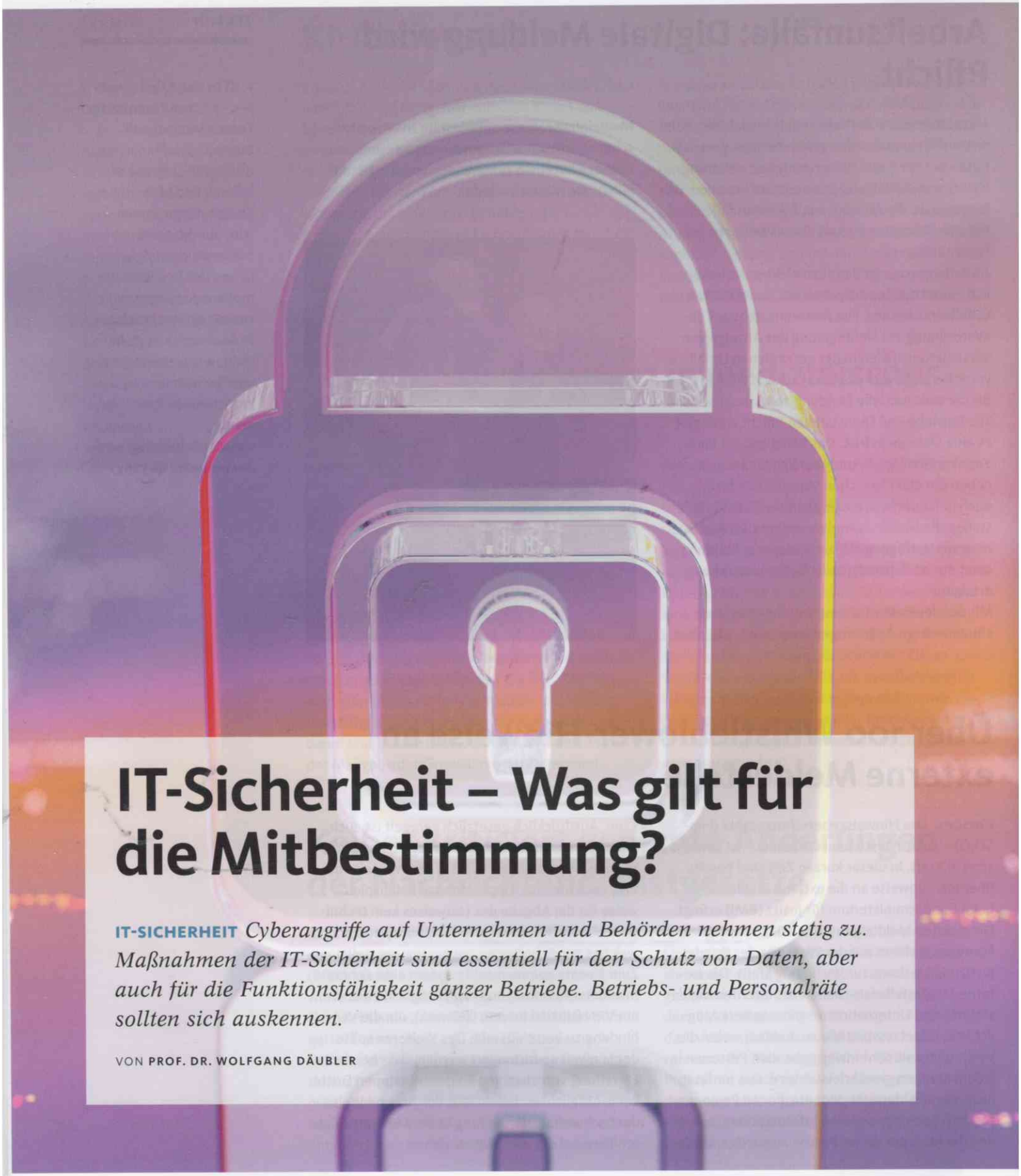

IT-Sicherheit – Was gilt für die Mitbestimmung?

IT-SICHERHEIT *Cyberangriffe auf Unternehmen und Behörden nehmen stetig zu. Maßnahmen der IT-Sicherheit sind essentiell für den Schutz von Daten, aber auch für die Funktionsfähigkeit ganzer Betriebe. Betriebs- und Personalräte sollten sich auskennen.*

VON **PROF. DR. WOLFGANG DÄUBLER**

Cyberangriffe haben in den letzten Jahren zugenommen. Das Bundeskriminalamt verzeichnete 2022 insgesamt 136.865 Fälle, doch sind diese nach seiner Einschätzung nur die Spitze des Eisbergs: Lediglich etwa ein Zehntel aller Fälle würden bekannt. Auch seien die aus dem Ausland kommenden Angriffe in der Statistik nicht erfasst.[1]

Was sind Cyberangriffe?

Eine verbreitete Angriffsform besteht darin, dass durch Schadsoftware das ganze System eines Unternehmens lahmgelegt wird und dieses anschließend eine »Mitteilung« erhält, bei Zahlung der Summe X (meist in Bitcoin) werde alles wieder freigeschaltet. Ebenfalls häufig ist sog. Phishing: Im Anhang einer harmlos aussehenden Mail der (angeblichen) Hausbank findet sich z. B. ein Fragebogen, in dem man »zu Verifikationszwecken« zahlreiche Kontodaten eintragen soll, die dann zum »Abräumen« des Kontos verwendet werden.[2] Es versteht sich von selbst, dass sich Unternehmen gegen solche Angriffe schützen wollen. Bei kritischer Infrastruktur kommt hinzu, dass bei Angriffen unter Umständen elementare Bedürfnisse der Bevölkerung nicht mehr befriedigt werden können: Wenn das Wasserwerk oder das Krankenhaus plötzlich ohne IT dasteht, kann dies verheerende Folgen haben. So geschehen in einem Krankenhaus in Neuss, welches fast einen Tag lang kein Zugriff auf die Systeme hatte, wodurch die Einsicht in Patientenunterlagen sowie die Vorbereitung und Durchführung von Operationen ausgeschlossen waren (siehe dazu Konrad-Klein, CuA 2/2017, 24).

Welche Sicherheitsvorkehrungen sind zu treffen?

Welche Schutzmaßnahmen zu ergreifen sind, ist im Einzelnen nicht rechtlich geregelt. Das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) enthält in den §§ 8a bis 8i lediglich allgemeine Vorgaben, die viel Konkretisierungsspielraum lassen. Außerdem gilt das BSI-Gesetz nur für die sog. kritische Infrastruktur wie Energieversorger, Krankenhäuser usw., nicht aber für alle Unternehmen (siehe Däubler, Digitalisierung und Arbeitsrecht, 8. Aufl. 2022, § 19 Rn. 5 ff., auch zum Folgenden).

Die übrigen Unternehmen orientieren sich an den (rechtlich nicht verbindlichen) ISO-Normen 27.001 ff. oder – wenn sie sich gegen IT-Risiken versichern wollen – an den Richtlinien der Versicherungswirtschaft. Man kann sich des Eindrucks nicht erwehren, dass die heute bestehende Rechtsordnung sehr viel mehr Wert auf die Sicherung personenbezogener Daten (Art. 32 DSGVO) legt als auf den Schutz der Allgemeinheit und den Schutz der Integrität von Unternehmen. Dies mag einer individualistischen Denkweise entspringen, die den »Dichter und Denker« und seine Persönlichkeit umfassend schützen will, ohne darauf zu achten, dass auch er wie alle anderen Menschen Lebensumstände braucht, in denen zumindest die »basic needs« wie Wasser, Strom, Wohnung und Nahrung gesichert sind.

Was gilt für die Mitbestimmung?

Für die Mitbestimmung des Betriebsrats und des Personalrats ergeben sich mehr Anwendungsmöglichkeiten, wenn keine zwingenden gesetzlichen Vorgaben vorhanden sind. Dabei hängt die Entscheidung, ob die Voraussetzungen eines Mitbestimmungsrechts gegeben sind, von den jeweiligen Umständen des Einzelfalls ab.

- Mitbestimmung bei Schulungen zum IT-Sicherheitsbewusstsein

Einschlägige Rechtsprechung ist bislang spärlich. Das Arbeitsgericht Düsseldorf hatte über einen Fall zu entscheiden, bei dem die Arbeitgeberin eine dreizehnminütige Schulung zum Sicherheitsbewusstsein »zum Schutze der IT« durchführen wollte (ArbG Düsseldorf, 5.3.2018 – 15 BV 38/18). Arbeitgeber und Betriebsrat waren sich einig, dass hierfür ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 1 BetrVG bestehe, was vom Arbeitsgericht Düsseldorf im Rahmen eines Verfahrens nach § 100 ArbGG bestätigt wurde. Auch das LAG Düsseldorf hatte als Beschwerdeinstanz insoweit keine Bedenken (LAG Düsseldorf, 8.5. 2018 – 3 TaBV 15/18). Die Mitbestimmung hätte auch bestanden, wenn die »Schulung« ein oder zwei Stunden gedauert hätte.

- Mitbestimmung bei Einführung eines Sicherheitsanalyse-Systems

DARUM GEHT ES

1. Cyberangriffe sind eine Gefahr für Unternehmen wie Behörden.

2. Es gehört nicht ausdrücklich zu den Aufgaben der Interessenvertretungen, für IT-Sicherheit zu sorgen.

3. Dennoch können Betriebs- und Personalrat im Rahmen der Mitbestimmung einiges bewirken.

1 https://www.tagesschau.de/inland/cyberangriffe-deutschland-bka-100.html (abgerufen am 10.11.2023)
2 Zum Phishing s. https://www.bundespolizei-virus.de/it-sicherheit/phishing/ (abgerufen am 10.11.2023)

Von grundsätzlicherer Bedeutung war demgegenüber eine Entscheidung des LAG München (23.7.2020 – 2 TaBV 126/19). Dabei ging es um den Einsatz des Sicherheitsanalyse-Systems »Securonix«, welches Abweichungen vom normalen Nutzungsverhalten, sog. Auffälligkeiten, erkennen kann.

Dabei werden Logdaten erfasst, die sich auf einzelne Mitarbeitende beziehen lassen. Die Auswertung kann ergeben, dass es sich um einen harmlosen Zufall handelte, der keine weitere Aufmerksamkeit erfordert. Es kann aber auch ein Ausnahmeverhalten vorliegen, das für sich allein kein erhöhtes Risiko indiziert, aber im Wiederholungsfall Relevanz gewinnt. Weisen Auffälligkeiten auf eine ernste Bedrohung hin, hat eine eingehende Untersuchung im Rahmen eines »Incident Management«-Prozesses zu erfolgen.

Das LAG München bejahte ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG, da das System geeignet war, Verhalten und Leistung von Arbeitnehmerinnen und Arbeitnehmern zu kontrollieren. In der Sache selbst wurde durch einen Mehrheitsbeschluss der mit dem Fall befassten Einigungsstelle der Einsatz des Systems gebilligt, weil zwar ein weitgehender Eingriff in die Persönlichkeitssphäre vorliege, dieser jedoch zur Schaffung von IT-Sicherheit geeignet und erforderlich sei und keine unverhältnismäßige Maßnahme darstelle.

Dies war insoweit bedenklich, als die betroffenen Beschäftigten nicht voll darüber aufgeklärt wurden, nach welchen Kriterien die erhobenen Daten ausgewertet, d. h. als »normal« oder »auffällig« qualifiziert wurden. Auch ist die Frage zu stellen, ob es nicht mildere Mittel gegeben hätte – beispielsweise eine stichprobenweise Erfassung –, die aus verfassungsrechtlichen Gründen den Vorrang gehabt hätten. Auch liegt der Sache nach eine Überwachung ohne konkreten Verdacht vor, was zumindest einer besonders starken Rechtfertigung bedarf (kritisch deshalb Wedde, jurisPR-ArbR 17/2021 Anm. 6).

▸ Was gilt nach dem BPersVG?

Aus der Personalvertretung sind keine einschlägigen Entscheidungen ersichtlich. Die Voraussetzungen für ein »Mitbestimmungsrecht« nach § 80 Abs. 1 Nr. 21 BPersVG sind keine anderen als die des § 87 Abs. 1 Nr. 6 BetrVG, doch kann die Einigungsstelle nach § 75 Abs. 3 BPersVG nur eine Empfehlung an die Oberste Dienstbehörde beschließen (weshalb das Wort »Mitbestimmungsrecht« auch in Anführungszeichen gesetzt ist). Immerhin besteht nach § 77 Abs. 2 Nr. 1 BPersVG ein Initiativrecht des Personalrats, das allerdings in dieselbe Sackgasse führt.

Was kann die Interessenvertretung tun?

Für IT-Sicherheit zu sorgen, ist keine ausdrücklich dem Betriebs- oder Personalrat zugewiesene Aufgabe. Dies hängt damit zusammen, dass es sich jedenfalls im Anwendungsbereich des BSI-Gesetzes primär um (auch) im Allgemeininteresse bestehende Sicherungsmaßnahmen handelt, die ähnlich wie im Polizeirecht dem öffentlichen Recht zugeordnet sind und ggf. durch Verwaltungsakt des Bundesamts für Sicherheit in der Informationstechnik (BSI) durchgesetzt werden können.

Das bedeutet allerdings nicht, dass eine betriebliche Interessenvertretung die Augen vor entsprechenden Gefahren schließen sollte. Die Situation ist insoweit keine andere als im Umweltrecht, das in der Betriebsverfassung bis 2001 ebenfalls keine Erwähnung fand, aber trotzdem im Rahmen der Qualifizierung nach § 37 Abs. 6 und 7 BetrVG als Schulungsgegenstand (ArbG Wiesbaden, 2.10.1991 – 7 BV 6/91; BAG, 11.10.1995 – 7 ABR 42/94) und im Rahmen des Bezugs von Zeitschriften nach § 40 BetrVG (LAG Frankfurt/Main, 21.3.1991 – 12 TaBV 191/90 zum Bezug der Zeitschrift »Arbeit & Ökologie-Briefe«) Bedeutung gewann.

Für den Betriebsrat wie für den Personalrat ergeben sich zwei Aufgabenfelder: Zum einen können sie Maßnahmen anregen, die der IT-Sicherheit dienen, zum anderen darüber wachen, ob Sicherungssysteme eingeführt werden, die ihre Mitbestimmung betreffen.

▸ Initiativen des Betriebs- oder Personalrats

Die Beschäftigten wissen häufig sehr viel besser als ihre obersten Chefs, wo Gefahren lauern können. Nach der Störfall-Verordnung (die insbesondere auf Chemie-Unternehmen Anwendung findet) müssen deshalb vor der Aufstellung eines Alarm- und Gefahrenabwehrplanes die Beschäftigten des betroffenen Betriebsbereichs angehört werden – ihr »Gefahrenwis-

sen« soll berücksichtigt werden (vgl. Kohte, in: Handkommentar BetrVG, 6. Aufl. 2022, § 87 Rn. 91). Betriebsrat und Personalrat können anregen, dass bei der IT-Sicherheit in gleicher Weise verfahren wird. Dabei können sie sich auf § 80 Abs. 1 Nr. 2 BetrVG bzw. § 62 Nr. 1 BPersVG stützen, wonach sie Maßnahmen beantragen können, die dem Betrieb bzw. der Dienststelle dienen – das kann unschwer auf die IT-Sicherheit bezogen werden. Eine solche Initiative setzt einen guten Informationsstand voraus – die §§ 80 Abs. 2 BetrVG bzw. 66 Abs. 1 BPersVG räumen der Interessenvertretung das Recht ein, alle Informationen zu erhalten, die sie zur Erfüllung ihrer Aufgaben benötigt. Die Initiative kann sich selbstredend nicht nur darauf beschränken, die Beschäftigten zu befragen; möglich sind auch Vorschläge zum Ankauf einer bestimmten Schutzsoftware und zur Schaffung eines Reserve-Servers, der neben dem offiziellen System steht und jeden Abend den neuesten Stand der Dinge speichert.

- Mitbestimmung bei der Einführung technischer Einrichtungen

Der Betriebsrat und der Personalrat werden außerdem darüber wachen, ob Sicherungssysteme eingeführt werden, die einzelne Mitbestimmungsrechte berühren. Sobald personenbezogene Daten betroffen sind, kommt das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG ins Spiel – dabei ist insbesondere zu prüfen, ob die geplante Maßnahme auf einer zwingenden gesetzlichen Vorgabe beruht oder ob der Arbeitgeber über Spielräume verfügt. Im Einzelfall kann auch § 87 Abs. 1 Nr. 1 BetrVG bzw. § 80 Abs. 1 Nr. 18 BPersVG berührt sein, weil z. B. bestimmte Regeln über das Verhalten im Betrieb aufgestellt werden, die sich nicht zwingend aus der Ausführung der Arbeit ergeben. Weiter ist auch an § 87 Abs. 1 Nr. 12 BetrVG bzw. § 80 Abs. 1 Nr. 14 BPersVG zu denken, die ein Initiativ- und Mitbestimmungsrecht bei Verbesserungsvorschlägen vorsehen. Warum sollten sich diese nicht auf die IT-Sicherheit erstrecken können?

Die Bestellung von IT-Sicherheitsbeauftragten

In vielen Betrieben wird ein »Informationssicherheitsbeauftragter« bestellt, der anders als der betriebliche Datenschutzbeauftragte keine Erwähnung im Gesetz gefunden hat (Eingehend dazu Däubler, in: Kipker (Hrsg.), Cybersecurity. Rechtshandbuch, 2. Aufl. 2023, Kap. 12 Rn. 113ff). Seine Aufgaben ergeben sich aus Regelwerken wie der ISO 27.002 oder dem BSI-Standard 200–2, die rechtlich nicht verbindlich sind, aber faktisch weithin befolgt werden. Im vorliegenden Zusammenhang interessiert, inwieweit der Betriebsrat bzw. Personalrat bei seiner Bestellung zu beteiligen ist.

Wird eine bisher im Betrieb beschäftigte Person als IT-Sicherheitsbeauftragte/r bestellt, so ändert sich damit ihr Tätigkeitsfeld. In der Regel liegt dann ähnlich wie bei der Bestellung zur oder zum betrieblichen Datenschutzbeauftragten eine Versetzung vor, die dem Betriebsrat ein Zustimmungsverweigerungsrecht nach § 99 Abs. 2 BetrVG gibt. Fehlt der betroffenen Person die nötige Fachkunde, wäre dies ein ausreichender Grund für ein »Nein«. Ein unzulässiger Interessenkonflikt würde vorliegen, wenn der oder die betriebliche Datenschutzbeauftragte zugleich IT-Sicherheitsbeauftragte/r werden soll: In der ersten Rolle hätte die fragliche Person dafür zu sorgen, dass möglichst wenige Daten erhoben und verarbeitet werden, in der zweiten Rolle bestünde Interesse an einer möglichst umfassenden Information über alles, was im Betrieb geschieht. Deshalb darf es hier keine »Personalunion« geben. In der Personalvertretung des Bundes ist die Situation grundsätzlich keine andere (hier gilt § 78 Abs. 1 Nr. 2 bis 6 BPersVG).

Fazit

Auch die IT-Sicherheit gehört zu den Aufgaben der Interessenvertretung. Betriebs- und Personalräte können hier einiges bewirken. Weil die Bedeutung der IT-Sicherheit immer größer wird, sollten sich Betriebs- und Personalräte intensiver darum kümmern. Soweit Maßnahmen auch personenbezogene Angaben zum Gegenstand haben, besteht in aller Regel ein Mitbestimmungsrecht. ◁

Prof. Dr. Wolfgang Däubler, Hochschullehrer i. R. für Arbeitsrecht, Bürgerliches Recht und Wirtschaftsrecht an der Universität Bremen.