Windows XP nach Support Ende

Ein rechtliches Risiko für Geschäftsführer, CIO und IT Dienstleister

Einführung:

Seit dem 8. April 2014 hat Microsoft offiziell und weltweit den Support für Windows XP beendet (nähere Informationen s. unter http://www.endofsupport.de). Mit wenigen Ausnahmen für Regierungsstellen und private Kunden, die ein entsprechendes Customer Support Agreement abgeschlossen haben und dafür teures Geld bezahlen müssen, kann somit kein Nutzer oder Reseller mehr von Microsoft irgendwelche Patches, Bug-fixes oder Sicherheitsupdates bekommen. Auch die Reseller und IT Serviceunternehmen haben weder Zugriff auf eine Serviceunterstützung oder Ansprechpartner von Microsoft noch auf den Quellcode der Software, sodass auch sie keine Reparaturen vornehmen können, sofern diese originär das System betreffen. Es bleibt lediglich die Möglichkeit, soweit möglich, durch externe Lösungen Work-arounds zu erstellen, die die unmittelbar in Windows auftretenden Probleme umgehen.

Dennoch hatten zum Zeitpunkt der Ankündigung laut Angaben von Net Applications immer noch 27 % aller Unternehmen weltweit ihre Software nicht umgestellt, sondern halten an dem „bekannten und bewährten“ Windows-XP-Standard fest. Neben der allzu menschlichen Weisheit „never change a running system“ stehen dahinter oftmals Überlegungen, die bei näherem Betrachten auf einfachen Fehleinschätzungen der rechtlichen Rahmenbedingungen beruhen, wie z. B.:

1.) „Solange keine Fehler sichtbar sind, ist alles in Ordnung.“
2.) „Wo im Gesetz steht, dass ich ein aktuelles Betriebssystem brauche?“
3.) „IT ist allein Sache des IT-Leiters, das betrifft den Geschäftsführer nicht.“
4.) „Dem Geschäftsführer/Aufsichtsrat kann nichts passieren.“
5.) „Wir sind doch versichert.“
6.) „Das ist Kundensache, dem Reseller/IT-Servicepartner kann das egal sein“.

Geschäftsleitung und IT-Leitung schieben sich gegenseitig die Verantwortung für das Thema zu, sehen die unmittelbar drohenden Risiken für ihr Unternehmen nicht oder glauben, dass es ihnen letztlich doch egal sein kann, solange nur alles vermeintlich funktioniert. Dabei ist es an der Zeit, mit einigen dieser Mythen endgültig aufzuräumen:

1. **Fehlglaube: „Wie alt oder aktuell unser Betriebssystem ist, ist doch egal, solange heute alles funktioniert.“**

In einer vernetzten Unternehmenswelt sind Angriffe auf die IT-Infrastruktur nicht mehr nur das Problem großer und prominenter Unternehmen. Im Gegenteil: gerade die oft nur unzureichend gewarteten Systeme kleinerer und mittlerer Unternehmen eignen sich hervorragend als Ziel für Angriffe auf deren Sicherheit. Moderne Hackerprogramme können von organisierten Banden ebenso wie von neugierigen Einzeltätern und sogar von Regierungsstellen unzulässig genutzt werden, um mit wenig Aufwand großflächig alle an das Internet angeschlossenen Systeme anzugreifen. Davon betroffen sind u. a. Webshops und die dort gespeicherten Kreditkartendaten der Kunden ebenso wie produzierende Unternehmen und ihre technischen Zeichnungen und Dokumentationen oder die Kunden- und Mitarbeiterdatenbanken aller Unternehmen. Gerade weit verbreitete Standardprogramme oder Betriebssysteme – zumal wenn ihnen wie bei Windows XP die Patchunterstützung fehlt - bieten sich dafür als Zielscheibe an, weil ihr hoher Verbreitungsgrad zugleich eine maximale Trefferwahrscheinlichkeit der Angriffe ermöglicht. Sobald eine Lücke in den Schutzmaßnahmen dieser Standardprogramme gefunden wurde, verbreitet sich die Neuigkeit in Windeseile in die entsprechende Szene und jeder, der darauf aus ist, versucht diese Lücke solange zu seinem Vorteil zu nutzen, wie sie noch nicht geschlossen wurde. Es drohen Datenverluste oder Manipulationen.

Zugleich setzen auf dem Betriebssystem zahlreiche andere Programme auf oder sind daran angebunden. Diese werden regelmäßig gewartet und erneuert. Es ist daher nur eine Frage der Zeit bis diese Programme nur noch in solchen Versionen verfügbar sind, die nicht mehr mit den alten Betriebssystemversionen (z. B. Windows XP) kompatibel sind. Wenn die aktuelle Applikationsumgebung nicht mehr auf das alte Betriebssystem passt, kann das zu einem Ausfall oder Nichtverfügbarkeit der neuen Sys-

teme und aller Funktionen führen, die mit diesen verbunden sind. Das entsprechende Schadensrisiko (z. B. durch einen Ausfall des Abrechnungssystems oder der Produktionssteuerung in der Industrie) ist erheblich.

Selbst wenn alle Programme also (noch) ohne sichtbare Ausfälle und scheinbar korrekt funktionieren, steigt das Risiko von Systemausfällen, Manipulationen oder Nichtverfügbarkeiten unternehmenskritischer Funktionen mit jedem Tag, an dem das Betriebssystem als wesentliche Basissoftware ohne Updates und Sicherheitsunterstützung des Herstellers bzw. der IT-Dienstleister auskommen muss. Niemand, der sich in der Verantwortung für eines dieser Risikoszenarien im Unternehmen sieht, kann daher ruhigen Gewissens den Sicherheits- und Wartungsstatus des Betriebssystems ignorieren.

2. Fehlglaube: „Die Aktualität des Betriebssystems ist eine technische (und maximal finanzielle) Frage; mit Gesetzen hat das nichts zu tun."

Es gibt in der Tat in Deutschland bisher kein Gesetz, das ausdrücklich Vorgaben für das Betriebssystem in der Unternehmens-IT macht. Allerdings haben alle Unternehmen in Deutschland, die zumindest auch personenbezogene Daten (z. B. ihrer Mitarbeiter, Kunden oder Zulieferer) elektronisch speichern, den **Datenschutz** zu beachten. Der wiederum konkretisiert in § 9 Bundesdatenschutzgesetz (BDSG) und der zugehörigen Anlage die technisch-organisatorischen Maßnahmen, die zum Schutz der Integrität der Daten und vor dem Risiko des Datenverlusts zu ergreifen sind. Und in diesem Zusammenhang verlangt das Gesetz ausdrücklich die Einhaltung des aktuellen Stands der Technik, wenn es um Maßnahmen der IT-Sicherheit geht.

Unternehmen der **Finanz- und Versicherungsbranche** haben zudem nach § 25a Kreditwesenkontrollgesetz (KWG) besondere organisatorische Pflichten für ein angemessenes und wirksames Risikomanagement einzuhalten. Dazu gehören u. a. eine angemessene organisatorisch-technische Ausstattung der Institute und die Einrichtung und Unterhaltung eines funktionierenden Notfallkonzepts, insbesondere für die IT-Systeme. Die Finanzbehörden haben zudem in entsprechenden Rundschreiben (MaRisk) die konkreten Standards festgeschrieben, die sie als Mindestausstattung für Finanz- und Versicherungsdienstleister erwarten. Ein veraltetes Betriebssystem, für das keinerlei Sicherheitsupdates oder Fehlerkorrekturen mehr verfügbar sind, erfüllt keinen dieser Standards. Kein Risikomanagement oder Notfallkonzept kann die Risiken, die aufgrund der fehlenden Wartbarkeit der Systeme drohen, effektiv eingrenzen.

Auch von solchen Unternehmen, die nicht der Finanzdienstleistungsaufsicht unterliegen, wird erwartet, dass sie eine **ausreichende Risikovorsorge** betreiben und die bestehenden Risiken für den Bestand des Unternehmens sorgfältig managen. Angriffe auf die Unternehmens-IT oder einfach nur unvorhergesehene Ausfälle des Systems können aufgrund der Bedeutung und Verzahnung der IT mit nahezu allen kritischen Unternehmensbereichen in vielen Fällen erhebliche Auswirkungen auf das Unternehmen haben. Sei es, dass die operative Leistungsfähigkeit des Unternehmens gefährdet ist, weil die Steuerungssoftware für eine Fertigungsstraße in der Industrie ausfällt, sei es, dass das Handelssystem zur Eingabe und Verarbeitung von Aufträgen und Rechnungen ausfällt und damit die Liquiditätslage des Unternehmens belastet wird.

Schließlich sind insbesondere die Belastungen zu sehen, die ein **Datenverlust** für die **Reputation des Unternehmens bei Kunden und Geschäftspartnern** zur Folge hat und die nur mit erheblichem finanziellen und öffentlichkeitswirksamen Aufwand wieder repariert werden kann. Gem. § 42a BDSG sind Unternehmen als verantwortliche Stelle gesetzlich verpflichtet, jeden unrechtmäßigen Zugriff oder Verlust von personenbezogenen Daten der Datenschutzaufsichtsbehörde anzuzeigen und in bestimmten Fällen auch die betroffenen Kunden oder Mitarbeiter direkt bzw. sogar über Presseanzeigen zu informieren. Versäumnisse in diesem Bereich führen zu hohen Bußgeldern.

Aus diesem Grund gehört das Vorhandensein einer sorgfältigen und gut dokumentierten Risikosteuerung in der IT gem. der Standards des Instituts der Wirtschaftsprüfer (IDW) - IDW PS 951 und 330 – zum Gegenstand der **Prüfungsaufgaben der Wirtschaftsprüfer** und muss von diesen im Jahresabschluss attestiert werden. Bei Unternehmen der

Versicherungs- und Finanzdienstleistungsbranche gehört dies sogar zu den Pflichtprüfungsbereichen der Wirtschaftsprüfer. Ist der Wirtschaftsprüfer nicht in der Lage, dem Unternehmen eine sorgfältige und risikogerechte IT-Organisation entsprechend dem aktuellen Stand der Technik zu bescheinigen, muss er zugleich das Testat für den Jahresabschluss verweigern. Ein nicht testierter Jahresabschluss kann jedoch eine verheerende Wirkung sowohl auf das Vertrauen der Geschäftspartner in die wirtschaftliche Stabilität des Unternehmens als auch insbesondere auf die **Kreditwürdigkeit des Unternehmens** haben. Banken und andere Kreditgeber sind nach den geltenden Regeln zur Kreditvergabe verpflichtet, einen testierten Jahresabschluss als wesentliches Kriterium für eine Kreditvergabe zu verlangen (Basel II Rating).

Den besonderen Risiken durch Cyberkriminalität will die Bundesregierung schließlich durch ein **IT-Sicherheitsgesetz** begegnen, das sie zur Cebit 2014 im Entwurf präsentiert hat und bis Ende 2014 in Kraft setzen möchte. Kernpunkt ist die Forderung, dass Betreiber von kritischen Infrastrukturen ebenso wie Telekommunikationsanbieter Mindestanforderungen an IT-Sicherheit zu erfüllen und erhebliche IT-Sicherheitsvorfälle dem Bundesamt für die Sicherheit in der Informationssicherheit (BSI) zu melden haben. Schutz- und Meldepflicht beschränken sich damit nicht mehr allein auf personenbezogene Daten, sondern auch auf sonstige unerlaubte Eingriffe in die IT-Infrastruktur. Darüber hinaus müssen auch alle Betreiber von kommerziellen Websites die Mindestanforderungen an IT-Sicherheit beachten und anerkannte Schutzmaßnahmen im zumutbaren Umfang umsetzen. Dazu gehört zumindest das Einspielen aktueller Sicherheitspatches und -updates, zu dem die Websitebetreiber nun ausdrücklich verpflichtet werden sollen.

3. Fehlglaube: „Betriebssysteme sind die Verantwortung der IT, das betrifft den Geschäftsführer nicht."

Die Gesellschaft hat ein hohes Interesse an einer funktionierenden, stabil aufgestellten und gesetzeskonform arbeitenden Wirtschaft. Aus diesem Grund verlangt der Gesetzgeber von allen Geschäftsführern und Vorständen der in Deutschland tätigen Unternehmen eine **sorgfältige und gesetzeskonforme Unternehmensführung** nach Maßgabe eines **ordentlichen und gewissenhaften Kaufmanns**. § 91 Abs. 2 Aktiengesetz (AktG) und § 43 Abs. 1 GmbH-Gesetz (GmbHG) verlangen dies nach herrschender Auffassung der Gerichte nicht nur von AG-Vorständen und GmbH-Geschäftsführern, sondern analog auch von allen Geschäftsführungen sämtlicher Unternehmensformen in Deutschland.

Es gehört daher zu den originären Aufgaben der guten Unternehmensführung, IT-Risiken mit Gefährdungspotential für das Unternehmen zu identifizieren, zu bewerten und die richtigen Maßnahmen zu deren Bekämpfung einzuleiten. Es geht dabei immer um die aktive Beeinflussung und Steuerung der IT-Risiken.

Natürlich kann nicht von jedem Geschäftsführer verlangt werden, sich in die Details der IT-Strukturierung einzuarbeiten. Er muss nicht selber die richtige Betriebssystem-Version einspielen. Aber der Geschäftsführer/Vorstand ist verpflichtet, die Einrichtung einer risikogerechten IT-Organisation anzuordnen und zu überwachen sowie durch richtige Auswahl, Anweisung und Überwachung der eingesetzten Personen und Maßnahmen für eine Gesetztestreue seines Unternehmens zu sorgen. Das bedeutet, er kann im Sinne einer arbeitsteiligen Unternehmensorganisation die Ausführung der IT-Organisation auf seinen IT-Leiter übertragen, die Verantwortung für diesen Bereich kann er jedoch nicht verlagern. Die Verantwortung verbleibt allein aufgrund seiner Zugehörigkeit zur Geschäftsführung immer bei ihm. Dies gilt im Übrigen für alle Mitglieder der Geschäftsführung gleichermaßen, selbst wenn diese die Geschäftsführungsbereiche untereinander aufgeteilt haben.

4. Fehlglaube: „Was soll mir als Geschäftsführer/IT-Leiter/Aufsichtsrat schon passieren?"

Gute Unternehmensführung gehört zu den originären Pflichten von **Geschäftsführern und Vorständen**. Fehler in diesem Bereich, die z. B. durch eine unzureichend gesicherte IT unmittelbare Schadensfolgen für das Unternehmen haben oder zu Bußgeldzahlungen für das Unternehmen führen, werden

diesem Personenkreis nach dem Gesetz unmittelbar und persönlich zur Last gelegt. Zugleich sinkt aufgrund prominenter Fälle in der Vergangenheit die Hemmung, solche Vorfälle auch tatsächlich zu verfolgen. Im vergleichbaren Fall der Einrichtung eines Anti-Korruptionsmechanismus verurteilte das Landgericht München I am 10.12.2013 z. B. ein ehemaliges Vorstandsmitglied von Siemens zur Zahlung von 15 Mio. Euro **Schadensersatz** (Az. 5HK O 1387/10), weil das Anti-Korruptionssystem lückenhaft war und die Ausführung nicht überwacht wurde.

Aufsichtsrat bzw. Verwaltungsrat des Unternehmens sind schließlich **persönlich haftbar** zu machen, wenn sie solche Verfehlungen des Vorstands und der Geschäftsführung nicht im Interesse des Unternehmens verfolgen und einklagen.

Das enthebt allerdings den **IT-Leiter** ebenso wenig wie jeden anderen leitenden Mitarbeiter mit Verantwortung für die IT vom Mitdenken und sorgfältigen Arbeiten. Gerade in einer arbeitsteiligen Unternehmensorganisation ist jeder Mitarbeiter verpflichtet, seine Vorgesetzten und damit letztlich auch die Geschäftsführung über Risikosituationen im Unternehmen zu informieren und bei deren Beseitigung seinen Beitrag zu leisten. Drohen daher durch ein nicht mehr gewartetes Betriebssystem wie Windows XP unmittelbare Sicherheitsrisiken für die Unternehmens-IT **haftet auch jeder verantwortliche Mitarbeiter im Rahmen der Begrenzungen des Arbeitsrechts persönlich für die rechtzeitige und vollständige Information der Geschäftsleitung**, damit diese die richtigen Konsequenzen ziehen kann.

5. Fehlglaube: „Wenn doch etwas passiert, zahlt ja die Versicherung."

Es wäre zumindest trügerisch, wenn sich Vorstände, Geschäftsführer und IT-Leiter darauf verlassen sollten, dass Fehler in der IT-Organisation, z. B. durch nicht rechtzeitige Aktualisierung des Betriebssystems und die damit verbundene Risikosteigerung für das Unternehmen, für sie persönlich keine Folgen haben, da sie ja möglicherweise in ihrer Geschäftsführertätigkeit über eine **Haftpflichtversicherung, eine sog. D&O (Directors & Officers) Versicherung**, abgesichert seien. Trügerisch ist dies deshalb, weil die meisten Standardbedingungen dieser Versicherungen einen Ersatz im Fall von grober Fahrlässigkeit ausschließen.

Nachdem in sämtlichen einschlägigen Medien – und nicht nur in der IT-Fachpresse – ausführlich über das Supportende für Windows XP berichtet wurde und zahlreiche Medienberichte insbesondere auf die möglichen Sicherheitsrisiken bei einem Weitereinsatz der Software hingewiesen haben, handelt jeder Geschäftsführer und Vorstand, der hierauf nicht reagiert, weit außerhalb der von ihm gesetzlich verlangten Sorgfaltspflichten und damit zunehmend auch grob fahrlässig. Er muss daher auch damit rechnen, dass ihm diese grobe Fahrlässigkeit von seiner Versicherung entgegengehalten wird.

6. Fehlglaube: „Das ist das Problem meiner Kunden, mir als Reseller/IT-Servicepartner kann das egal sein."

Jeder **Reseller oder IT-Servicepartner**, der einen aktiven Wartungs- oder Servicevertrag mit seinem Kunden hat, muss ein ureigenstes Interesse daran haben, dass sein Kunde keine Software einsetzt, für die der Hersteller, wie bei Windows XP, die Unterstützung eingestellt hat.

Zunächst liegt es auf der Hand, dass der Servicepartner, der selber keinen Zugriff auf den Windows-XP-Quellcode hat, auf die Unterstützung des Herstellers angewiesen ist, wenn er entsprechend seinem Wartungsvertrag mit dem Kunden dort eines der oben geschilderten Probleme beheben soll. Stellt der Kunde eine Sicherheitslücke in der vom Servicepartner betreuten Software fest, ist der Servicepartner zur Behebung verpflichtet, kann dafür aber nicht auf die Unterstützung des Herstellers zurückgreifen. Im Einzelfall lassen sich solche Situationen vielleicht mit „Work-arounds" beheben. Ein dauerhafter und stabiler Systembetrieb ist auf diese Weise aber nicht sicherzustellen. Der Servicepartner wird somit unweigerlich und absehbar in einen **Vertragsbruch seines Wartungsvertrages** hineingeraten und zumindest seinen Anspruch auf die Wartungsvergütung für diesen Leistungsteil verlieren. Unter bestimmten Umständen kann es zudem sein, dass er für entstandene Schäden des Kunden aufkommen muss.

Ein solches Schadensrisiko ist insbesondere dann zu befürchten, wenn der Servicepartner sich zugleich auch noch ein **Beratungsverschulden** vorwerfen lassen muss. Die Rechtsprechung geht davon aus, dass ein Servicepartner, dem sich der Kunde insbesondere aufgrund seiner versprochenen technischen Kompetenz und seiner Kenntnis der Microsoft-Lizenzsituationen anvertraut hat, verpflichtet ist, nicht nur reaktiv auf Serviceanfragen des Kunden zu reagieren und z. B. Wartungstickets zu beheben. Er hat vielmehr zumindest auch die **vertragliche Nebenpflicht, den Kunden aktiv auf bestehende Sicherheitslücken und Risiken hinzuweisen**. Der Kunde kann sich in diesem Zusammenhang im Verhältnis zu dem Servicepartner auf dessen Fachkenntnis verlassen und dessen Einschätzung zur Notwendigkeit eines Softwareupgrades vertrauen. Analog zur oben dargestellten Verantwortlichkeit der IT-Leiter und Geschäftsführer des Kunden können diese sogar durch sorgfältige Auswahl und Überwachung eines Servicepartners ihre eigene Verantwortung für mögliche Schäden auf den Servicepartner „delegieren“, wenn sie keinen Anlass hatten, seiner Empfehlung bezüglich der Migration oder Nicht-Migration zu misstrauen.

Rät der Servicepartner allerdings aktiv zur Ablösung von Windows XP, wobei er dem Kunden die möglichen Sicherheitsrisiken (s. o.) aufzeigt und erläutert, muss er sich keinen Vorwurf machen lassen, wenn sich der Kunde dennoch gegen die Ablösung entscheidet oder trotz wiederholtem Hinweis untätig bleibt. In diesem Zusammenhang kommt es dann darauf an, dass der Servicepartner z. B. durch entsprechende Gesprächsprotokolle oder Schreiben dokumentieren kann, dass er seiner Beratungspflicht nachgekommen ist. Nur wer für eine **ausreichende Dokumentation der aktiven und umfassenden Beratung** sorgt, kann davon ausgehen, im Falle eines Falles von der Haftung gegenüber dem Kunden verschont zu bleiben.

Fazit:
Der Einsatz unsicherer, nicht getesteter oder nicht mehr unterstützter Software wie Windows XP gefährdet die Sicherheit der Unternehmens-IT, da man damit rechnen muss, dass es Eindringlingen oder schadhaften Angriffen viel zu leicht gemacht wird, auf diese IT-Systeme zuzugreifen. Die Verantwortung für dieses Risiko trägt in erster Linie die Geschäftsführung des betroffenen Unternehmens, also der Geschäftsführer oder Vorstand. Er kann diese Verantwortung auch nicht an seine Mitarbeiter oder Dienstleister delegieren. Zugleich trifft aber auch die Mitarbeiter mit Verantwortung für die IT die wichtige Pflicht aus ihrem Arbeitsverhältnis heraus, die Geschäftsführung auf dieses Risiko hinzuweisen und entsprechende Gegenmaßnahmen zu ergreifen. Gleiches gilt für externe IT-Servicepartner, die aufgrund der Beratungssituation gegenüber dem Kunden eine erhebliche Verantwortung für deren Lizenzsituation und ggf. sogar eine aktive Hinweispflicht haben können. Rechtsprechung und Gesetzgeber geben hier keine Freifahrtscheine und nur, wenn jeder der Beteiligten sich seiner Verantwortung bewusst ist und diese erst nimmt, lassen sich die Risiken für das Unternehmen vermeiden. Das Recht lässt den Unternehmen völlig freie Hand, wie sie die Sicherheitsrisiken beheben (z. B. ob mit einem Upgrade oder auch Systemwechsel). Untätigkeit oder Gleichgültigkeit gegenüber dem Risiko wird hingegen unmittelbar bestraft und kann für die Betroffenen drastische Folgen haben.

Dr. Matthias Orthwein, LL.M. (Boston)

Dr. Matthias Orthwein, LL.M. ist Rechtsanwalt und Partner bei SKW Schwarz Rechtsanwälte in München.
Dr. Matthias Orthwein, LL.M. berät nationale und internationale Mandanten im IT-Recht, vor allem im Softwarerecht bspw. bei Lizenzrechtsauseinandersetzungen, beim Entwurf und der Verhandlung von Softwareerstellungs- und -kaufverträgen. Er ist Lehrbeauftragter für IT- und Datenschutzrecht an der Hochschule Rosenheim.

Impressum

SKW Schwarz
Rechtsanwälte Steuerberater Wirtschaftsprüfer Partnerschaft mbB

Sitz der Partnerschaft ist München,
eingetragen beim Amtsgericht München PR 884.
Vertretungsberechtigter: Prof. Dr. Mathias Schwarz

redaktionell verantwortlich: Dr. Matthias Orthwein
E-Mail: m.orthwein@skwschwarz.de
im Auftrag von: Microsoft Deutschland GmbH

80333 München
Wittelsbacherplatz 1
T +49 (0) 89.286 40-0
F +49 (0) 89.280 94 32

Gesetzliche Berufsbezeichnung: Rechtsanwalt/-anwältin der BRD.
Zuständige Rechtsanwaltskammer: Rechtsanwaltskammern Berlin, Düsseldorf, Frankfurt/Main, Hamburg und München.

Die berufsrechtlichen Regelungen sind unter http://www.brak.de in der Rubrik „Berufsrecht“, Informationspflichten gem. § 5 TMG abrufbar.

SKW Schwarz Rechtsanwälte ist eine unabhängige deutsche Anwaltskanzlei mit über 100 Anwälten an fünf Standorten. SKW Schwarz berät Unternehmen von inhabergeführten Firmen bis zu börsennotierten Aktiengesellschaften sowie Privatmandanten auf allen wesentlichen Gebieten des nationalen und internationalen Wirtschaftsrechts.