APPELHAGEN

NIS2 – für wen gilt sie?
Und was ist noch von der EU zu erwarten?

9. Fachkonferenz Cybersicherheit, 12.09.2024

APPELHAGEN

Jens Stanger

- Rechtsanwalt
- Fachanwalt für Informationstechnologierecht

- IT-Recht, eCommerce, Datenschutzrecht.

- Unternehmen aus der IT-Branche.
- Unternehmen aus dem Mittelstand, öffentliche Auftraggeber.

- Softwareverträge.
- eCommerce-Projekte.

APPELHAGEN

Über uns

- 32 Rechtsanwälte, Steuerberater und Notare
- 80 qualifizierte Mitarbeiter
- Braunschweig
- Mitglied der Integrated Advisory Group (IAG International)

iag Integrated Advisory Group International

JUVE

NOMINIERT JUVE AWARDS 2012 Kanzlei des Jahres Für den Mittelstand

APPELHAGEN

Portfolio

- Rechtliche Beratung,
  Prozessführung und Gestaltung
- Steuerberatung
- Betriebswirtschaftliche Beratung
- Notariat

APPELHAGEN

NIS-2-Richtlinie
Network and **I**nformation **S**ecurity

Ziel:

- Festlegen von Maßnahmen zur Herstellung eines hohen gemeinsamen Cybersicherheitsniveaus in der gesamten Union.

- Mindestharmonisierung.

APPELHAGEN

NIS-2-Richtlinie
Network and **I**nformation **S**ecurity

Maßnahmen:

- Pflicht zur Registrierung (Art. 3 Abs. 4).
- Pflicht zur Umsetzung von „Cybersicherheitsrisikomanagementmaßnahmen“ und Meldung erheblicher Sicherheitsvorfälle (Art. 4).
- Cybersicherheitsrisikomanagement (Art. 21).
- Berichtspflichten (Art. 23).
- Austausch von Cybersicherheitsinformationen (Art. 29 - freiwillig).

APPELHAGEN

Wen betrifft's?

1. **Zugehörigkeit zu einem bestimmten Sektor bzw. Teilsektor**
   - Kritische Infrastruktur
   - In **Anhang 1** NIS-2-RL aufgeführte Unternehmen
   - In **Anhang 2** NIS-2-RL aufgeführte Unternehmen

2. **Bestimmte Unternehmensgröße**

   → **Mittlere Unternehmen**

   (in Abgrenzung zu „kleinen Unternehmen“ und „Kleinstunternehmen“)

APPELHAGEN

Wen betrifft's?

„wesentliche Einrichtung“ (EU)
„besonders wichtige Einrichtung“ (DE)

- Betreiber kritischer Anlagen (Kritis-VO)
- Unternehmen
  - genannt in **Anlage 1** BSI-Gesetz
  - mit min. 250 Mitarbeitern oder
  - Jahresumsatz von über 50 Mio. € **oder** Jahresbilanzsumme über 43 Mio. €.
- […]

„wichtige Einrichtung“ (EU & DE)

- Unternehmen
  - genannt in **Anlagen 1 oder 2** BSI-Gesetz
  - mit min. 50 Mitarbeitern **oder**
  - Jahresumsatz von über 10 Mio. € **oder** Jahresbilanzsumme über 43 Mio. €.

APPELHAGEN

Die Anlagen der NIS-2-RL oder des BSI-Gesetzes

Anlage 1 (Sektoren)

- Energie
- Transport und Verkehr
- Finanzwesen
- Gesundheit
- Wasser
- Digitale Infrastruktur
- Weltraum

Anlage 2

- Transport und Verkehr (Kurierdienste)
- Abfallbewirtschaftung
- Produktion, Herstellung und Handel m. chemischen Stoffen
- Produktion, Verarbeitung und Vertrieb von Lebensmitteln
- Verarbeitendes Gewerbe/Herstellung von Waren
  - Datenverarbeitungsgeräte, elt. & opt. Erzeugnisse
  - Elektrische Ausrüstungen
  - Maschinenbau
  - Kraftwagen und Kraftwagenteile
  - Sonstiger Fahrzeugbau
- Anbieter digitaler Dienste
- Forschung

APPELHAGEN

Anlage 2 NIS-2-RL
Verarbeitendes Gewerbe/Herstellung von Waren: Maschinenbau

5. Verarbeitendes Gewerbe/Herstellung von Waren	a) Herstellung von Medizinprodukten und In-vitro-Diagnostika	Einrichtungen, die Medizinprodukte im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates [4] herstellen, und Einrichtungen, die In-vitro-Diagnostika im Sinne des Artikels 2 Nummer 2 der Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates [5] herstellen, mit Ausnahme der unter Anhang I Nummer 5 fünfter Gedankenstrich dieser Richtlinie aufgeführten Einrichtungen, die Medizinprodukte herstellen
	b) Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 26 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	c) Herstellung von elektrischen Ausrüstungen	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 27 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	d) Maschinenbau	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 28 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	e) Herstellung von Kraftwagen und Kraftwagenteilen	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 29 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	f) sonstiger Fahrzeugbau	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 30 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben

APPELHAGEN

Anlage 2 NIS-2-RL
Verarbeitendes Gewerbe/Herstellung von Waren: Maschinenbau

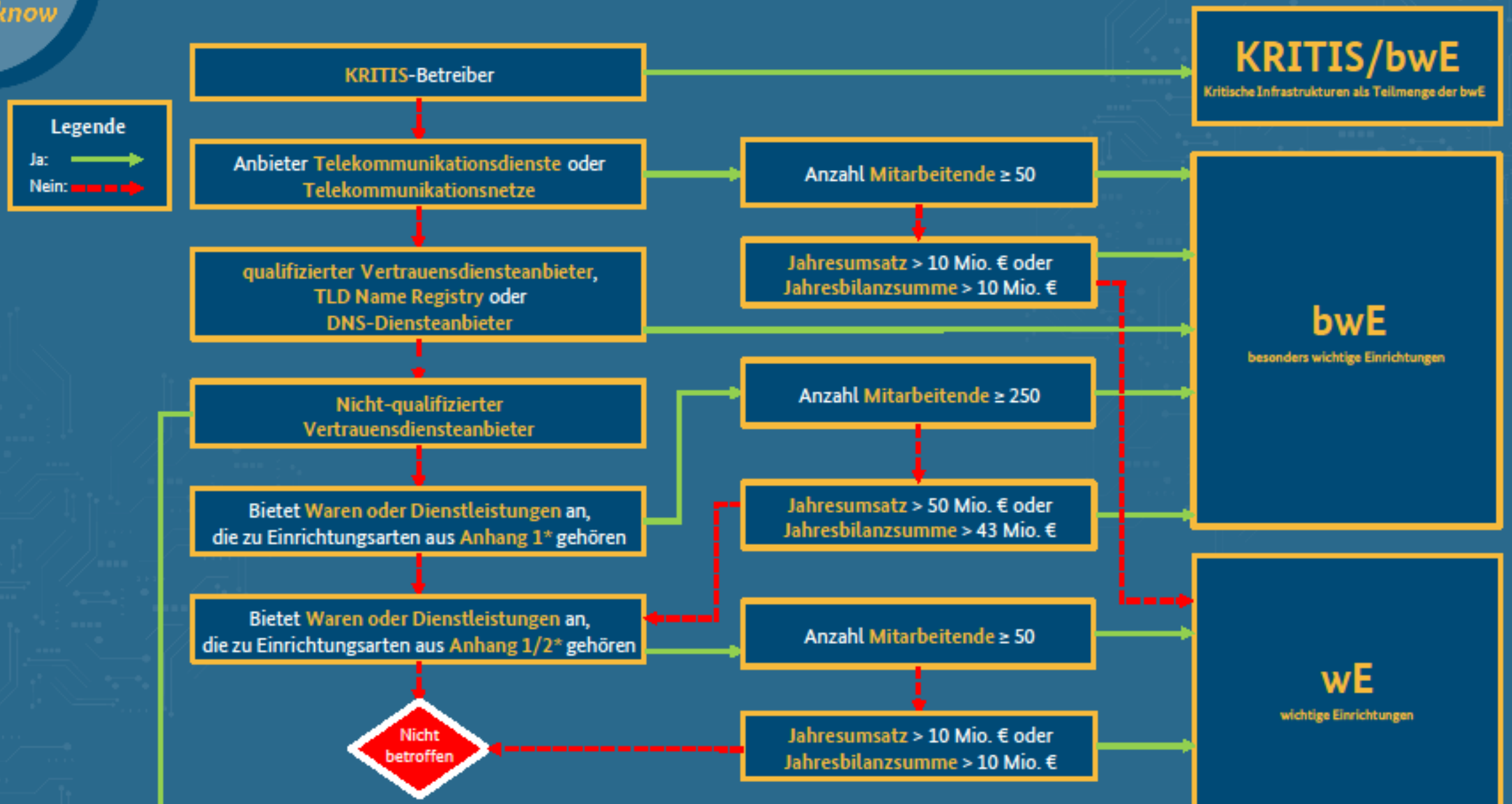
5. Verarbeitendes Gewerbe/Herstellung von Waren	a) Herstellung von Medizinprodukten und In-vitro-Diagnostika	Einrichtungen, die Medizinprodukte im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates [4] herstellen, und Einrichtungen, die In-vitro-Diagnostika im Sinne des Artikels 2 Nummer 2 der Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates [5] herstellen, mit Ausnahme der unter Anhang I Nummer 5 fünfter Gedankenstrich dieser Richtlinie aufgeführten Einrichtungen, die Medizinprodukte herstellen
	b) Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 26 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	c) Herstellung von elektrischen Ausrüstungen	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 27 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	d) Maschinenbau	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 28 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	e) Herstellung von Kraftwagen und Kraftwagenteilen	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 29 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	f) sonstiger Fahrzeugbau	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 30 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben

APPELHAGEN

Statistische Systematik der Wirtschaftszweige in der Europ. Gemeinschaft NACE Rev. 2

a. n. g.: anderweitig nicht genannt				*Teil von
Abteilung	Gruppe	Klasse		ISIC Rev. 4
28			Maschinenbau	
	28.1		Herstellung von nicht wirtschaftszweigspezifischen Maschinen	
		28.11	Herstellung von Verbrennungsmotoren und Turbinen (ohne Motoren für Luft-und Straßenfahrzeuge)	2811
		28.12	Herstellung von hydraulischen und pneumatischen Komponenten und Systemen	2812
		28.13	Herstellung von Pumpen und Kompressoren a. n. g.	2813*
		28.14	Herstellung von Armaturen a. n. g	2813*
		28.15	Herstellung von Lagern, Getrieben, Zahnrädern und Antriebselementen	2814
	28.2		Herstellung von sonstigen nicht wirtschaftszweigspezifischen Maschinen	
		28.21	Herstellung von Öfen und Brennern	2815
		28.22	Herstellung von Hebezeugen und Fördermitteln	2816
		28.23	Herstellung von Büromaschinen (ohne Datenverarbeitungsgeräte und periphere Geräte)	2817
		28.24	Herstellung von handgeführten Werkzeugen mit Motorantrieb	2818
		28.25	Herstellung von kälte-und lufttechnischen Erzeugnissen, nicht für den Haushalt	2819*
		28.29	Herstellung von sonstigen nicht wirtschaftszweigspezifischen Maschinen a. n. g.	2819*

#nis2know



*Anhang 1: www.bsi.bund.de/dok/nis-2-anhang-1 | Anhang 2: www.bsi.bund.de/dok/nis-2-anhang-2

APPELHAGEN

Hilfe im Internet

Der Gesetzestext:

https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/CI1/nis2umsucg.html

Anhang I: https://www.bsi.bund.de/dok/nis-2-anhang-1

Anhang II: https://www.bsi.bund.de/dok/nis-2-anhang-2

BSI: NIS-2-Betroffenheitsprüfung

https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Betroffenheitspruefung/nis-2-betroffenheitspruefung_node.html

BSI: NIS-2-Entscheidungsbaum

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/NIS-2/nis-2-betroffenheit-entscheidungsbaum.html?nn=1115626

NACE Rev. 2

https://ec.europa.eu/eurostat/documents/3859598/5902453/KS-RA-07-015-DE.PDF

APPELHAGEN

„Cybersicherheitsrisikomanagementmaßnahmen“

§ 30 BSI-Gesetz (Reg.-Entwurf 22.07.2024)

- **Abs. 1**
  Pflicht, „geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen, […] zu ergreifen,
  um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten.

- **Abs. 2**
  Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen. ***Die Maßnahmen müssen zumindest Folgendes umfassen:[…]***

APPELHAGEN

„Cybersicherheitsrisikomanagementmaßnahmen“

Art. 21 Abs. 2 NIS-2-RL, § 30 BSI-Gesetz (Reg.-Entwurf 22.07.2024)

Maßnahmen müssen mindestens Folgendes umfassen:

- **Konzepte** in Bezug auf die **Risikoanalyse** und auf die Sicherheit in der Informationstechnik,
- Bewältigung von **Sicherheitsvorfällen**,
- Aufrechterhaltung des Betriebs, wie **Backup-Management und Wiederherstellung** nach einem Notfall, und Krisenmanagement,
- **Sicherheit der Lieferkette** einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,
- Sicherheitsmaßnahmen bei **Erwerb, Entwicklung und Wartung** von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,

APPELHAGEN

„Cybersicherheitsrisikomanagementmaßnahmen“

Art. 21 Abs. 2 NIS-2-RL, § 30 BSI-Gesetz (Reg.-Entwurf 22.07.2024)

- Konzepte und Verfahren zur **Bewertung der Wirksamkeit** von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
- grundlegende Verfahren im Bereich der Cyberhygiene und **Schulungen** im Bereich der Sicherheit in der Informationstechnik,
- Konzepte und Verfahren für den **Einsatz von Kryptografie** und Verschlüsselung,
- Sicherheit des Personals, Konzepte für die **Zugriffskontrolle** und für das Management von Anlagen,
- Verwendung von Lösungen zur **Multi-Faktor-Authentifizierung** oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

APPELHAGEN

Schulungspflicht der Geschäftsleitung
Art. 20 Abs. 2 NIS-2-RL

*„Die Mitgliedstaaten stellen sicher, dass **die Mitglieder der Leitungsorgane wesentlicher und wichtiger Einrichtungen an Schulungen teilnehmen müssen**, und fordern wesentliche und wichtige Einrichtungen auf, allen Mitarbeitern regelmäßig entsprechende Schulungen anzubieten, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.“*

APPELHAGEN

Was dürfen Sie noch von der EU erwarten?

Regelung	Regelt	Betroffene Akteure	Geltung ab
Digital Operational Resilience Act (DORA)	Stellt sicher, dass Finanzunternehmen ihre IT-Systeme widerstandsfähig gegenüber Störungen und Cyberangriffen machen.	Banken, Versicherungen, Vermögensverwalter, Zahlungsdienstleister, kritische Dienstleister für Finanzsektor.	17. Januar 2025
Cyber Resilience Act	Beinhaltet Cybersicherheitsanforderungen für vernetzte Produkte und IoT-Geräte.	Hersteller, Importeure, Händler von vernetzten Geräten und Software in der EU.	Frühestens ab 2024 (geplant)
KI-Act	Legt Vorschriften für die Entwicklung und Nutzung von Künstlicher Intelligenz fest, mit Fokus auf Risikobewertung.	Unternehmen, die KI-Anwendungen entwickeln oder einsetzen, insbesondere bei Hochrisikoanwendungen (z. B. in Medizin, Verkehr).	Noch nicht in Kraft (geplant für 2025 oder später)

APPELHAGEN

Was liegt Ihnen noch am Herzen?

APPELHAGEN

Vielen Dank
für Ihre Aufmerksamkeit

APPELHAGEN Rechtsanwälte Steuerberater PartGmbB · Theodor-Heuss-Straße 5a · 38122 Braunschweig
Telefon +49 (531) 28 20-0 · Telefax +49 (531) 28 20-5 25 · info@appelhagen.de · www.appelhagen.de

APPELHAGEN

Maßstab für Beratung.