Die Cyberversicherung im Lichte der NIS2-Richtlinie

Anforderungen und Erwartungen an den Versicherungsschutz

WOLTER HOPPENBERG
Rechtsanwälte Partnerschaft mbB

Ausgangslage der NIS2-Richtlinie laut Gesetzentwurf v. 02.10.2024

- Infolge des völkerrechtswidrigen russischen Angriffskriegs auf die Ukraine hat sich nach Einschätzung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) im Bericht zur Lage der IT-Sicherheit in Deutschland 2023 die IT-Sicherheitslage insgesamt zugespitzt.

- Im Bereich der Wirtschaft zählen hierbei Ransomware-Angriffe, Ausnutzung von Schwachstellen, offene oder falsch konfigurierte Online-Server sowie Abhängigkeiten von der IT-Lieferkette und in diesem Zusammenhang auch insbesondere Cyberangriffe über die Lieferkette (sog. Supply-Chain-Angriffe) zu den größten Bedrohungen

- Hacktivismus, insbesondere mittels Distributed-Denial-of-Service (DdoS)-Angriffen oder auch durch in Deutschland erfolgte Kollateralschäden infolge von Cyber-Sabotage-Angriffen im Rahmen des Krieges

- Zunahme von Störungen und Angriffen im Bereich der Lieferketten sowohl aus den Bereichen Cybercrime als auch im Rahmen des Krieges

- Diese Phänomene treten nicht mehr nur vereinzelt auf, sondern sind insgesamt Teil des unternehmerischen Alltags geworden

- Eine Erhöhung der Resilienz der Wirtschaft gegenüber den Gefahren der digitalen Welt ist daher eine zentrale Aufgabe für die beteiligten Akteure in Staat, Wirtschaft und Gesellschaft, um den Wirtschaftsstandort Deutschland und den Binnenmarkt der Europäischen Union insgesamt robust und leistungs- und funktionsfähig zu halten

Etablierung eines unionsweiten Mindestniveaus an Cybersicherheit durch die NIS2-Richtlinie

Maßnahmen zur IT- und Cybersicherheit

„Stand der Technik“ als Knackpunkt, da Technik und Bedrohungen im stetigen Wandel sind

Inhaltskern

- Bedrohungslage mit häufigen Verweisen auf den Krieg zwischen Russland und der Ukraine
- Stetiger Zuwachs der Bedrohungen
- Missstände benannt (DdoS-Angriffe)
- Ziel: Resilienz der Wirtschaft

AVB Cyber

- Im April 2017 hatte der Gesamtverband der Versicherer e. V. (GDV) erstmals unverbindliche Musterbedingungen für die Cyberrisiko-Versicherung veröffentlicht. Damals bereits existierende Versicherungskonzepte konzentrierten sich in erster Linie auf den industriellen Bereich. Die Musterbedingungen sollten auch den Bereich kleiner und mittelständischer Unternehmen erfassen.
- Aber: weiter heterogenes Angebot am Markt, keine Konsolidierung
- Problem: gerichtliche Entscheidungen haben oft nur Einzelfallcharakter

Obliegenheiten des VN

Der Versicherungsnehmer ist zu technisch-organisatorischen Schutzmaßnahmen verpflichtet.
Welches Schutzniveau?
Die Maßnahmen müssen dem „Stand der Technik“ entsprechen.

AVB Cyber 2024, neue Fassung

- **IT-Sicherheitsniveau**: Die vom versicherten Unternehmen zu erfüllenden Obliegenheiten wurden neu formuliert, um den aktuellen technischen Stand abzubilden und das Verständnis beim Leser zu verbessern. Die Basis für ein angemessenes IT-Sicherheitsniveau bilden weiterhin die bekannten, einfach umzusetzenden Maßnahmen wie regelmäßige Datensicherungen, starke Passwörter, individuelle Zugänge, Virenscanner, Firewalls und schnell installierte Sicherheitsupdates.

A1-16 Obliegenheiten vor Eintritt des Versicherungsfalls zur Gewährleistung der IT-Sicherheit
Der Versicherungsnehmer hat vor Eintritt des Versicherungsfalls alle vertraglichen Obliegenheiten einzuhalten.

A1-16.1
Dazu gehört insbesondere, dass die informationsverarbeitenden Systeme

a)einzelne Nutzer und Befugnisebenen unterscheiden. Hierzu sind individuelle Zugänge für alle Nutzer erforderlich. Es ist technisch sicherzustellen, dass Passwörter bestimmte Mindestanforderungen erfüllen (insbes. Anzahl der Zeichen). Administrative Zugänge sind ausschließlich Administratoren und ausschließlich zur Erledigung administrativer Tätigkeiten vorbehalten.

b)mit einem zusätzlichen Schutz gegen unberechtigten Zugriff ausgerüstet sind, wenn diese einem erhöhten Risiko ausgesetzt sind.

Ein erhöhtes Risiko besteht

–bei Geräten, die über das Internet erreichbar sind (Server) oder

–bei Mobilgeräten.

Zusätzliche Schutzmaßnahmen für Geräte, die über das Internet erreichbar sind (Server) können z.B. sein: Firewall, 2-Faktor-Authentifizierung bei Servern.

Zusätzliche Schutzmaßnahmen für Geräte, die über das Internet erreichbar sind (Server) können z.B. sein: Firewall, 2-Faktor-Authentifizierung bei Servern.

Schutzmaßnahmen für mobile Geräte wie Smartphones oder Laptops können z.B. sein: Verschlüsselung von Datenträgern mobiler Geräte, Diebstahlsicherung oder ähnlich wirksame Maßnahmen.

c)über einen Schutz gegen Schadsoftware verfügen, dessen Schutzniveau automatisch auf dem aktuellen Stand gehalten wird (z.B. Virenscanner, Code Signing, Application Firewall oder ähnlich wirksame Maßnahmen);

d)einem Patch-Management-Verfahren unterliegen, das eine zeitnahe Installation von relevanten Sicherheitsupdates sicherstellt, die ein Risiko für die Sicherheit der informationsverarbeitenden Systeme des Versicherungsnehmers reduzieren. Systeme und Anwendungen mit bekannten Sicherheitslücken dürfen nicht ohne zusätzliche geeignete Maßnahmen zur Absicherung eingesetzt werden, die das Risiko einer Ausnutzung der Sicherheitslücken und eines Schadens effektiv minimieren.

e)einem mindestens wöchentlichen Sicherungsprozess unterliegen und es ist sicherzustellen, dass kein System und keine Befugnisebene Schreibberechtigung auf Originale und Duplikate hat und diese gleichermaßen verändern oder vernichten kann.

Geeignete Maßnahmen können beispielsweise sein,

-bei lokalen Backups von Einzelplatzrechnern: Regelmäßige physische Trennung des Backup-Mediums, Überschreiben des Backup-Mediums sind nur mit administrativem Zugriff möglich;

bei Backups über das Netzwerk: Die gesicherten Geräte dürfen keine Befugnis haben, Sicherungskopien zu löschen; Sofern ein einheitliches Managementsystem verwendet wird (bspw. active directory) darf der Back-up-Server nicht in dieses Managementsystem eingebunden sein.

Der Versicherungsnehmer hat eine ordnungsgemäße Funktion des Sicherungs- und Wiederherstellungsprozesses durch regelmäßige Prüfung nach einem festgelegten Turnus sicherzustellen.

A1-16.2
Darüber hinaus hat der Versicherungsnehmer

a)alle **gesetzlichen**, behördlichen sowie vertraglich vereinbarten **Sicherheitsvorschriften** einzuhalten;

b)besonders gefahrdrohende Umstände auf Verlangen des Versicherers innerhalb angemessener Frist zu beseitigen. Dies gilt nicht, soweit die Beseitigung unter Abwägung der beiderseitigen Interessen unzumutbar ist. Ein Umstand, der zu einem Schaden geführt hat, gilt ohne weiteres als besonders gefahrdrohend.

Obliegenheiten in den AVB Cyber

- Besondere Obliegenheiten nach A1.16.1
- Einzeln aufgeführt und im Zweifelsfall Inhalt der Regelung durch Auslegung zu ermitteln.

- Allgemeine Obliegenheiten nach A1.16.2
- Einhaltung von Sicherheitsvorschriften
- U.a. durch **Gesetze**: NIS2!

NIS2 vom Regelungszweck erfasst?

Es muss sich um Vorschriften handeln, die gerade der Verhütung der mit der Obliegenheit bekämpften Gefahr dienen (vgl. auch BGH r+s 2002, 292). Das ist bei der Cyberversicherung bei Vorschriften der Fall, die dem **Schutz personenbezogener Daten** (z. B. DS-GVO, § 88 TKG) oder dem **Schutz kritischer Infrastruktur vor Cyberangriffen** (§ 8a BSI-Gesetz) dienen

Damit wird der **NIS2-**Inhalt auch von A1.16.2 erfasst sein.

„Stand der Technik“ Gesetzesgrundlage

- Im Cyber-Sicherheitsrecht kommt dem Begriff des Stands der Technik aufgrund der schnellen Entwicklungszyklen eine besondere Bedeutung zu. Die Verwendung wird genutzt, um das erforderliche Sicherheitsniveau flexibel und technikneutral zu gewährleisten.

- Die Notwendigkeit der Einhaltung eines hohen Sicherheitsniveaus folgt aus dem Umstand, dass die Digitalisierung in nahezu allen Bereichen des täglichen Lebens von hoher Dynamik geprägt ist und sich somit auch die Verfahren, Einrichtungen und Betriebsweisen der IT–Sicherheit ständig weiterentwickeln.

- Gleichzeitig führt diese hohe Dynamik dazu, dass die jeweilige Bestimmung des „Stands der Technik” zu einem konkreten Zeitpunkt eine besondere Herausforderung darstellt. Dies erfordert einen kontinuierlichen Prozess, der regelmäßig geprüft und angepasst werden muss.

- Bisher geregelt in § 8 und § 8 a BSIG mit Verweis auf Einhaltung „ Stand der Technik“

- § 13 Abs. 7 TMG

- Art. 32 Abs. 1 DS–GVO

- NIS-2-Richtlinie: Indem sie den Stand der Technik berücksichtigen, können Organisationen und Betreiber sicherstellen, dass sie effektiv auf die sich ständig ändernden Herausforderungen der Cyber-Sicherheit reagieren und ihre Systeme und Daten angemessen schützen.

- Dies ist ein zentraler Bestandteil der Anforderungen der NIS-2-Richtlinie, die ein hohes Sicherheitsniveau in der gesamten Europäischen Union gewährleisten soll

Aber möglicherweise unterschiedliche Adressaten KRITIS und Adressaten der NIS2-Richtlinie müssen nicht deckungsgleich mit dem VN sein

Ist der „Mindeststandard“ dann zu hoch?

Adressaten der NIS2-Richtlinie

- Öffentliche Verwaltung
- Digitale Dienste
- Post- und Kurierdienste,
- Abfallbewirtschaftung, Chemikalien- und Lebensmittelproduktion (einschließlich der Verarbeitung und des Vertriebs)
- Herstellung von medizinischen und elektronischen Produkten, Maschinen und Fahrzeugen
- KMU-Schwellenwerte für kleine und mittlere Unternehmen

Verpflichtungen?

-Registrierungspflicht

-vorfallabhängigen Meldepflichten

-ein umfassendes, auch die Lieferkette abdeckendes Risikomanagement, um Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit von IT-Systemen, Komponenten und Prozessen zu vermeiden und Auswirkungen von Sicherheitsvorfällen gering zu halten

-Haftung des Leitungsorgans gegenüber dem Unternehmen für den Fall einer unzureichenden Implementierung.

Anforderungen zudem aus „DORA“

- Gilt für Finanzunternehmen
- Unternehmen, die den Finanzunternehmen digitale Dienste und Datendienste einschließlich Hardwaredienstleistungen zur Verfügung stellen (sog. IKT-Drittdienstleister)

- dezidierte und feingliedrige Anforderungen an das IKT-Risikomanagement
- Auch hier Verantwortung des Leitungsorgans

Unterschiedliche Anforderungen je nach VN?

- Ja!
- Die besonderen Obliegenheiten betreffen den jeweiligen VN unter Bezugnahme des Sicherheitsniveaus des versicherten Unternehmens.
- Die allgemeinen Obliegenheiten beziehen die geltende Gesetzeslage in den Versicherungsschutz ein. Dabei entfaltet das Gesetz für den VN nur dann eine Wirkung (Laut AVB „Einhaltung von Sicherheitsvorschriften“), wenn er auch Adressat des Gesetzes ist.
- IT- und Sicherheitsanforderungen können daher zu unterschiedlichen Ergebnissen führen

Unterschiedliche Ergebnisse auch bei der Subsumtion

- **Besondere Obliegenheiten**

- Müssen ggf. durch Auslegung ermittelt werden. Dabei kommt es auf das Verständnis eines durchschnittlichen VN an.
- Unbestimmte Rechtsbegriffe zu Lasten des Versicherers

- Allgemeine Obliegenheiten

- Gesetze dürfen **unbestimmte Rechtsbegriffe** enthalten. Dann ggf. durch Auslegung zu ermitteln, aber keine eingeschränkte Auslegungsperspektive wie bei den Versicherungsbedingungen.

Bedeutung Stand der Technik im Cyber-Sicherheitsrecht?

Die dynamische Risikoentwicklung im Bereich der Cyber-Angriffe hat insbesondere in den letzten Jahren bei Versicherern zu erhöhten Anforderungen und Mindestkriterien geführt, die Unternehmen für den Abschluss einer Deckung erfüllen müssen.

Ziel ist es, eine gute Cyber-Hygiene und Resilienz zu fördern, welche maßgeblichen Einfluss auf die Eintrittswahrscheinlichkeit und Schadenhöhe von Cyber-Schäden haben kann.

Dabei unterscheiden sich die Mindestanforderungen je nach Umsatz und Branche des Unternehmens.

Weiter Möglichkeit: Auflagen in der Cyberversicherung

Versicherer können Versicherungsschutz an Auflagen koppeln, die der VN zu erfüllen hat.

Auflagen als Anforderung zu Informationssicherheit

- Beispiele:

1. Back-Up,
2. Patch-Management
3. MFA für Fernzugriffe
4. End of Life Systeme
5. Durchführung einer Phishing Kampagne
6. Cyber Incident Response (Notfallpläne)

Teilweise mit Umsetzungfrist, und Meldungserfordernis an Versicherer

Auflagen als vorvertragliche Anzeigenpflichtverletzung, Obliegenheitsverletzung, Risikoauschluss

Die unterschiedliche Bewertung führt zu unterschiedlichen Beweisanforderungen und Ergebnissen. Ein Ausschluss lässt automatisch den Versicherungsschutz entfallen, eine Obliegenheitsverletzung nur mit zusätzlichen Voraussetzungen, wie Kausalität, Verschulden, fristgerechte Kündigung.

Unterschied AVB und Individualvereinbarung

AVB unterliegen, anders als ausgehandelte Individualvereinbarungen, einer strengen gesetzlichen Inhaltskontrolle und sind anhand des Verständnisses eines durchschnittlichen VN auszulegen.
Eine Individualvereinbarung kann daher für den VN von Nachteil sein.

Weiteres Thema: Bußgelder

Umstrittenes Thema: Auslegung von Kriegsausschlusses

- **Krieg und staatliche Angriffe**: Die Neufassung der AVB stellt klar, dass ein Krieg im Sinne der Bedingungen nicht den Einsatz physischer Waffengewalt voraussetzt. Schäden durch Kriegshandlungen sind auch dann **ausgeschlossen**, wenn der **Krieg mit digitalen Mitteln** geführt wird. Darüber hinaus formulieren die neuen Musterbedingungen einen Ausschluss für **staatliche Cyberangriffe**. Demnach sind Schäden ausgeschlossen, die eine direkte oder indirekte Folge eines erfolgreichen staatlichen Angriffs auf kritische Infrastrukturen sind.
- Auslegungsspielräume sind damit beseitigt.

Zurück zum Willen des Gesetzgebers:

Ausgangslage der NIS2-Richtlinie laut Gesetzentwurf v. 02.10.2024

- Infolge des völkerrechtswidrigen russischen Angriffskriegs auf die Ukraine hat sich nach Einschätzung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) im Bericht zur Lage der IT-Sicherheit in Deutschland 2023 die IT-Sicherheitslage insgesamt zugespitzt.

- Im Bereich der Wirtschaft zählen hierbei Ransomware-Angriffe, Ausnutzung von Schwachstellen, offene oder falsch konfigurierte Online-Server sowie Abhängigkeiten von der IT-Lieferkette und in diesem Zusammenhang auch insbesondere Cyberangriffe über die Lieferkette (sog. Supply-Chain-Angriffe) zu den größten Bedrohungen

- Hacktivismus, insbesondere mittels Distributed-Denial-of-Service (DdoS)-Angriffen oder auch durch in Deutschland erfolgte Kollateralschäden infolge von Cyber-Sabotage-Angriffen im Rahmen des Krieges

- Zunahme von Störungen und Angriffen im Bereich der Lieferketten sowohl aus den Bereichen Cybercrime als auch im Rahmen des Krieges

- Diese Phänomene treten nicht mehr nur vereinzelt auf, sondern sind insgesamt Teil des unternehmerischen Alltags geworden

- Eine Erhöhung der Resilienz der Wirtschaft gegenüber den Gefahren der digitalen Welt ist daher eine zentrale Aufgabe für die beteiligten Akteure in Staat, Wirtschaft und Gesellschaft, um den Wirtschaftsstandort Deutschland und den Binnenmarkt der Europäischen Union insgesamt robust und leistungs- und funktionsfähig zu halten

Mit der Klarstellung in der Kriegsausschlussklausel auf den Einbezug von Cyberangriffen, die vom Staat ausgehen, wäre der Versicherungsschutz zu versagen.

Aber: Der Versicherer trägt die Beweislast. In der Praxis regelmäßig nicht nachzuweisen, dass es sich um einen staatlichen Angriff handelt

Aber es gibt hier Beweiserleichterungen für den Versicherer:

Gemäß A1-17.2 lit. b) Satz 2 AVB-Cyber sollen die Voraussetzungen des Risikoausschlusses für staatliche Angriffe insbesondere dann vorliegen, wenn eine IT-forensische Untersuchung der informationsverarbeitenden Systeme des VN oder bei der Informationssicherheitsverletzung verwendeter Systeme oder Hilfsmittel **objektive Hinweise auf die Beteiligung, Urheberschaft oder Steuerung der Informationssicherheitsverletzung durch einen Staat, im Auftrag oder unter Kontrolle eines Staates ergeben**.
Ein solcher objektiver Hinweis soll unter anderem vorliegen, wenn **eine Beteiligung von Gruppen oder Personen nachgewiesen werden kann, die in der Vergangenheit bereits an entsprechenden Handlungen des Staates beteiligt waren** (vgl. A1-17.2 lit. b) Satz 3 AVB-Cyber). Voraussetzung für das Vorliegen eines objektiven Hinweises in diesem Sinne wäre folglich eine Beteiligung von Gruppen oder Personen, denen eine Mitwirkung an einem staatlichen Cyberangriff auf kritische Infrastrukturen in der Vergangenheit nachgewiesen wurde und die nachweislich auch an der Verursachung einer Informationssicherheitsverletzung beim VN im konkreten Fall beteiligt waren.

Bußgelder nach NIS2

- Die AVB Cyber sehen in A1.17.11. einen Ausschlusstatbestand für behördliche Maßnahmen, Strafen und Bußgelder vor.
- Damit wird die herrschende Meinung, dass jedenfalls nach deutschem Recht verhängte Geldstrafen und Geldbußen nach **§ 138 Abs. 1 BGB** nicht versicherbar sind, weil der Versicherungsschutz den gesetzlichen Präventionszweck vereiteln würde.
- Damit kann eine Inanspruchnahme des Versicherers nach einem NIS2-Bußgeld nicht erfolgen. Es ist aber davon auszugehen, dass nach einem verhängten Bußgeld auch ein solcher Tatbestand vorliegen dürfte, der eindeutig für eine Obliegenheitsverletzung des VN spricht.

Konsequenzen der NIS2-Richtlinie für die Cyberversicherung

- Sicherheitsanforderungen der NIS2-Richtlinie gelten auch als Obliegenheiten des VN, sofern er Adressat der Regelung ist.
- Dabei können unbestimmt Rechtsbegriffe auch zu Lasten des VN gelten.
- Bußgelder nach NIS2 sind weiterhin nicht versichert.
- Der Kriegsausschluss wird zunehmend Bedeutung haben, was einen begrenzten Versicherungsschutz durch die Cyberversicherung bedeutet.

Ihre Ansprechpartnerin

Francesca Kerkloh, LL.M.
Rechtsanwältin

+49 2381 92122-417

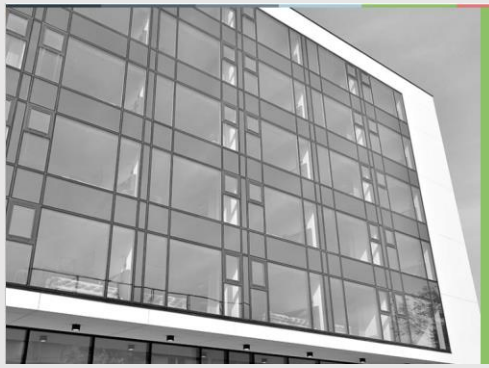
+49 151 19547728

+49 2381 92122-7102

kerkloh@wolter-hoppenberg.de

Kompetenzen

Informieren Sie sich gern über unsere Kompetenzen durch einen auf die jeweilige Expertise



Öffentliche Hand

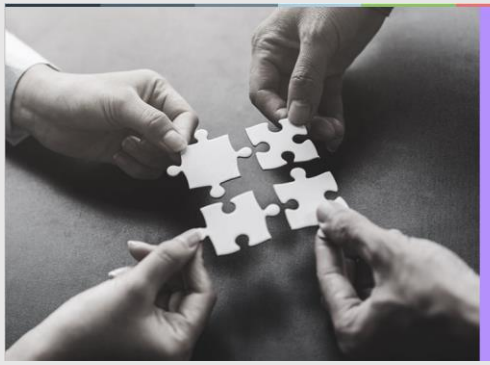
Antworten auf alle Fragestellungen der öffentlichen Hand aus einer Hand.

Mittelstand

Maßgeschneiderte Lösungen für Unternehmensgründungen, Umwandlungen und komplexe Projekte

Notariat

Ihr Ansprechpartner in allen notariellen Angelegenheiten



Spezialmaterien

Auch in Spezialfragen sind Sie bei uns in guten Händen.

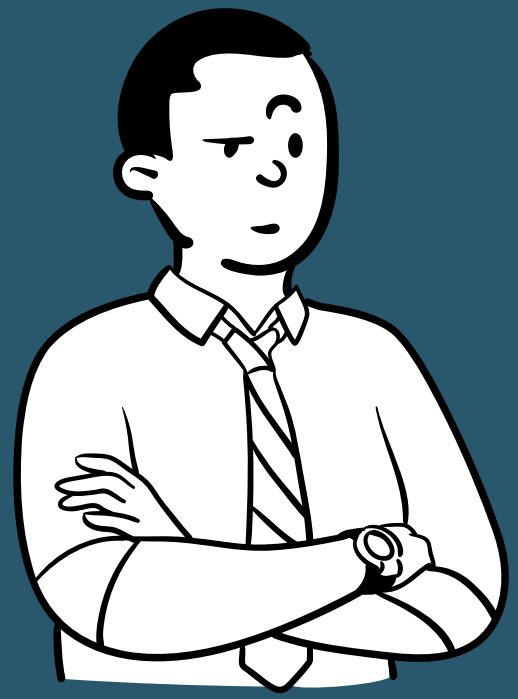
WOLTER HOPPENBERG

Seit 100 Jahren beraten und vertreten wir Mandanten der öffentlichen Hand und der mittelständischen Wirtschaft

Mit mehr als **60 Anwälten** (davon vier Notare) und Steuerberatern sind wir bundesweit tätig

Wir sind an den Standorten **Hamm** (Westf.), **Berlin**, **Köln, Münster** und **Osnabrück** vertreten

Wir stehen für fachlich und strategisch exzellente Lösungen, die in der Praxis Bestand haben



Die Präsentation dient Ihrer Information. Sie enthält keine Rechtsberatung.

Sollten Sie Teile oder die gesamte Präsentation für eigene Zwecke nutzen wollen oder Rückfragen haben - sprechen Sie uns gerne an.

Die Präsentation dient Ihrer Information. Sie enthält keine Rechtsberatung.

Sollten Sie Teile oder die gesamte Präsentation für eigene Zwecke nutzen wollen oder Rückfragen haben - sprechen Sie uns gerne an.

HAMM

Telefon: +49 2381 92122-0
Telefax: +49 2381 92122-7000

Münsterstr. 1-3
59065 Hamm

BERLIN

Telefon: +49 30 26390059-0
Telefax: +49 30 26390059-655

Bernburger Straße 32
10963 Berlin

KÖLN

Telefon: +49 221 272686-0
Telefax: +49 221 272686-955

Apostelnkloster 17-19
50672 Köln

MÜNSTER

Telefon: +49 251 9179988-0
Telefax: +49 251 9179988-855

Hafenweg 14
48155 Münster

MÜNSTER

Telefon: +49 251 9179988-0
Telefax: +49 251 9179988-89

Fridtjof-Nansen-Weg 3a
48155 Münster

OSNABRÜCK

Telefon: +49 541 506967-0
Telefax: +49 541 506967-699

Möserstraße 2-3
49074 Osnabrück