CYBER-SICHERHEIT

WIR HELFEN IHNEN, IHR UNTERNEHMEN ZU SCHÜTZEN

www.mazars.de

Wirtschaftsprüfung
Steuerberatung
Accounting & Outsourcing
Rechtsberatung
Financial Advisory Services
Consulting

MAZARS

Roever Broenner Susat Mazars

CYBER-SICHERHEIT

EINE HERAUSFORDERUNG FÜR IHR UNTERNEHMEN

THEMA CYBER-SICHERHEIT
Eine Herausforderung für Ihr Unternehmen 04

CYBER-SICHERHEIT BEGINNT BEIM VORSTAND 05

ÜBERPRÜFUNG DER CYBER-RISIKEN UND DES PROGRAMMS 06

DIE CYBER-SICHERHEIT IST NUR SO STARK WIE DAS SCHWÄCHSTE GLIED EINER ORGANISATION 07

NUTZEN SIE DIE CLOUD?
Sind Sie sich der möglichen Risiken und Vorteile bewusst? 09

CYBER ESSENTIALS UND CYBER ESSENTIALS PLUS 10

IST IHR UNTERNEHMEN GEGEN EINE SICHERHEITSVERLETZUNG GESCHÜTZT? 11

WARUM MAZARS? 12

ANSPRECHPARTNER 13

STANDORTE 16

THEMA CYBER-SICHERHEIT

Eine Herausforderung für Ihr Unternehmen

Unternehmen und Finanzinstitute haben die technologische Entwicklung der letzten 10 Jahre dazu genutzt, die Digitalisierung voranzutreiben: Digitalisierung in Form von Dienstleistungen am Kunden als auch digitale Neustrukturierung interner Prozesse. Mit der komplexen Technologie der Digitalisierung entstehen ständig neue Sicherheitsanforderungen; es wird immer schwerer, das wertvolle geistige Eigentum und die digitalen Unternehmensinformationen gegen Diebstahl und Missbrauch zu schützen.

Unternehmen müssen vorbereitet sein auf die Abwehr externer (Hacker, „Hacktivisten" und staatlich finanzierte Angriffe) sowie interner Angriffe (z.B. durch verärgerte Angestellte). Sogar in großen und gut geschützten Unternehmen kommt es fast täglich zu einer Verletzung der Cyber-Sicherheit. Wir alle kennen aus den Medien etliche bekannte Sicherheitsverstöße. Cyberangriffe haben weitreichende wirtschaftliche Folgen für Unternehmen: neben den rein finanziellen auch rufschädigende und juristische Auswirkungen. Keine Branche ist dagegen immun. Sicherheitsverletzungen sind für viele Einrichtungen fast schon zur „Normalität" geworden.

Da diese Sicherheitsverletzungen anhalten, wurde das Thema Cyber-Sicherheit zu einem der Anliegen für Investoren, Vorstände und Prüfungsausschüsse.

In unserer immer stärker Technologie-zentrierten Welt müssen die Risiken für Unternehmen aus externen oder internen Quellen zunächst verstanden und effizient gesteuert werden, wenn sie überwunden werden sollen.

CYBER-SICHERHEIT BEGINNT BEIM VORSTAND

Was Mazars für Sie tun kann

Die Cyber-Sicherheitsexperten von Mazars bieten umfassende Schulungen für Mitglieder des Vorstands und Prüfungsausschusses an, die auf den Entwicklungsstand des Unternehmens zugeschnitten sind. Folgende Inhalte sind vorgesehen:

→ Grundverständnis schaffen: Welche jüngsten Cyber-Bedrohungen könnten Ihr Unternehmen treffen?

→ Rollenverständnis schärfen: Welche Rollen und Verantwortlichkeiten des Vorstands und Prüfungsausschusses in Bezug auf Cyber-Sicherheit sind nötig?

→ Expertenwissen vermitteln: Was bedeutet Cyber-Sicherheit für Sie als Vorstand in Bezug auf Risikomanagement?

→ Gemeinsam planen: Wie bewerten Sie Ihren Cyber-Sicherheitsstatus momentan? Wie kann der Zielzustand definiert werden?

Jedes Unternehmen ist heutzutage angewiesen auf Informationen, die von zunehmend differenzierten Systemen und einer Technologie unterschiedlicher Herkunft erzeugt werden. Diese immer mehr verflochtene „Cyber-Welt" macht es nach Ansicht von Investoren und Regulierungsbehörden erforderlich, die Aufsichtspflicht von Vorständen in Bezug auf Cyber-Risiken offenzulegen. Sie müssen die Hauptprobleme rund um Cyber-Sicherheit einschätzen und bewährte Vorgehensweisen übernehmen können. Dabei geht es nicht nur um Risikomanagement, sondern auch um Aufdeckung.

Immer mehr Mitglieder aus Vorständen und Prüfungsausschüssen betrachten mittlerweile Cyber-Sicherheitsrisiken als Teil des unternehmensweiten Risikomanagements (ERM). Es gibt jedoch immer noch Geschäftsführer und Mitarbeiter mit Aufsichtsfunktion, die das Thema Cyber-Risiko für ein reines IT-Problem halten.

Zahlreiche Umfragen bestätigen, dass das Cyber-Risiko für Vorstände zu den größten Risiken gehört. Aber das Verständnis der tatsächlichen Auswirkungen für ihr Unternehmen – was den guten Ruf, die Rechtslage oder Lieferketten angeht – ist nicht unbedingt ausreichend.

ÜBERPRÜFUNG DER CYBER-RISIKEN UND DES PROGRAMMS

Was Mazars für Sie tun kann

Mazars unterstützt Unternehmen und Finanzinstitute bei der Bewertung ihrer Cyber-Sicherheitsprogramme und Belastbarkeit (Resilienz). Mazars verfügt über ein eigenes geschütztes Tool, das einen maßgeschneiderten Ansatz, bewährte Methoden und einige Rechtsprechungen berücksichtigt:

UNSER LÖSUNGSANSATZ IN 4 SCHRITTEN:

1. Überprüfung des eigenen Risikoprofils bezüglich Organisation, Technologie, Vertriebskanal und externem Umfeld
2. Bestimmung der Cyber-Sicherheitsniveaus des Unternehmens/Instituts nach den folgenden fünf Faktoren: Identifizierung, Schutz, Aufdeckung, Reaktion und Behebung.
3. Bewertung der entscheidenden Kontrollen
4. Ausarbeitung eines Plans zur pragmatischen Umsetzung des gewünschten Sicherheitsniveaus

Regulierungsbehörden drängen weltweit auf höhere Kompetenz bei Cyber-Sicherheit, gerade bei entscheidender Infrastruktur wie Finanzinstitute oder Energieversorger (siehe EU-NIS Richtlinie von Anfang 2016). Unternehmen müssen ihr Cyber-Sicherheitslage verbessern und über Compliance hinausgehen.

Cyber-Risiken sollten als integraler Bestandteil des aktuellen ERM-Prozesses, der Strategie zur Informationssicherheit und Geschäftskontinuität sowie des Supply Chain Managements sein.

Organisationen und Finanzinstitute beziehen Cyberrisiken tendenziell in die oben genannten Prozesse ein, passen aber ihr Cyber-Programm nicht zwangsläufig an die Geschäftsrisiken an und verfehlen damit das Ziel der Belastbarkeit (Resilienz).

Eine Resilienz-Strategie stellt sicher, dass Informationen angemessen geschützt werden. Sie garantiert zudem, dass Investitionen in die Sicherheit die richtigen Ziele verfolgen und gewünschten Nutzen bringen.

DIE CYBER-SICHERHEIT IST NUR SO STARK WIE DAS SCHWÄCHSTE GLIED EINER ORGANISATION

Was Mazars für Sie tun kann

MAZARS UNTERSTÜTZT UNTERNEHMEN BEI DER RISIKOBEWERTUNG INNERHALB DER LIEFERKETTE:

→ Welcher Bewertungsrahmen für zuverlässige Lieferanten ist für Sie der richtige? Wie ist die Sicherheit während der Due Diligence-Phase und als fortlaufender Prozess einzuschätzen?

→ Wie effizient sind die Sicherheitspraktiken der Lieferanten, wobei die von den Lieferanten ausgefüllten Fragenbögen kritisch zu hinterfragen sind?

→ Wie sind das Zulieferer-Risikomanagement und seine Wirksamkeit zu beurteilen?

→ Wie ist die kontinuierliche Überwachung der bewährten Zulieferer zu bewerten?

In den letzten Jahren stellt sich als das schwächste Glied meistens die Lieferanten heraus. Der Kreditkartenbetrug im Fall des amerikanischen Einzelhändlers Target zeigt, wie leicht ein Milliarden schwerer Konzern durch einen Zulieferer (ein Klimaanlagen-Betreiber) gefährdet werden kann, nur aufgrund von schwachen IT Sicherheitsverfahren.

Im letzten Jahrzehnt hat sich Outsourcing weit verbreitet. Dabei werden sensible Informationen und der IT-Zugang externen Beteiligten zur Verfügung gestellt. Zulieferer und Partner mit einem Zugang zu firmeneigenen IT-Netzwerk und Daten, sollten auf das mögliche Risiko für den Informationsschutz des Unternehmens hin bewertet und klassifiziert werden.

In der Praxis stellte sich dies als sehr schwierig heraus: Wie lässt sich der Sicherheitsstatus des Zulieferers objektiv messen? Alle Abteilungen, die mit der Lieferkette zu tun haben – von der Rechtsabteilung über den Einkauf bis zur Informationssicherheit - sollten gemeinsam ein Sicherheitsprogramm entwickeln. Nur so kann das Informationsrisiko ausreichend abgedeckt werden. Sowohl die Häufigkeit als auch der Aufwand der Sicherheitsbewertung sollten dem Risikograd entsprechen. Für ein Vertrauen in die Lieferkette sollte sich ein risikobasierter, transparenter und flexibler IT-Sicherheitsansatz von allen Beteiligten zu eigen gemacht werden.

DIE WICHTIGSTEN SCHRITTE ZUR INFORMATIONSSICHERHEIT

1	**BESTANDSAUFNAHME** Führen Sie eine Bestandsaufnahme aller IT-Assets durch und lokalisieren Sie diese
2	**KLASSIFIKATION** Klassifizieren Sie das Verkäufer/Partner-Risiko
3	**VEREINBAHRUNG** Nehmen Sie die IT-Sicherheitsanforderungen und Zusicherung in die Vereinbarungen mit auf
4	**TEAM** Bilden Sie die Verkäufer aus und üben Sie
5	**KONTROLLE** Überprüfen und überwachen Sie die IT-Sicherheitsprogramme der Verkäufer
6	**BEFRAGUNG** Befragen Sie den Verkäufer/Partner zu seiner Informationssicherheit
7	**LÖSUNGSORIENTIERT.** Wir erarbeiten Lösungen für Sie, die praxisnah und pragmatisch sind.
8	**WIR VERTRETEN WERTE.** Sie bekommen höchste Dienstleistungsqualität zu fairen Preisen.
9	**ANSPRECHBAR UND ERREICHBAR.** Wir wollen für Sie erreichbar sein. Das hat oberste Priorität.

DIE WICHTIGSTEN SCHRITTE ZUR INFORMATIONSSICHERHEIT

Betroffene: Verkäufer, Partner, Rechtsabteilung, Beschaffung/Einkauf, IT, Compliance

1.
Erstellung einer Liste der IT-Assets am Standort

2.
Einstufung des Verkäufer-/Partnerrisikos

3.
Integration von IT-Sicherheitsanforderungen und Versicherungen in Vereinbarungen

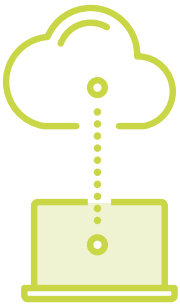
4.
Schulung der Verkäufer

5.
Test und Überwachung der IT-Sicherheitsprogramme von Verkäufern

6.
Befragung des Verkäufers/Partners zu seiner IT-Sicherheit

NUTZEN SIE DIE CLOUD?

Sind Sie sich der möglichen Risiken und Vorteile bewusst?



Cloud Computing ist das neue Eldorado der Unternehmenschefs, die sich in Richtung schnellere und kundenorientierte Systeme weiterentwickeln wollen. Dieser Trend wird noch verstärkt durch Unternehmen, die ihre Technologiekosten und Gefährdungspotenzial verringern möchten. Dies geschieht durch Übernahme der „Cloud first"- Strategie (von der Regierung des Vereinigten Königreichs 2011 verabschiedet). Dabei wird die Cloud als gutes Mittel wahrgenommen, um Kontinuitätsrisiken auszulagern. Ziele sind die Reduzierung der Stillstandszeiten auf Null und Schaffung eines sicheren Umfeldes bei gleichzeitigen Kostenvorteilen.

Während einige Risiken abgeschwächt werden, entstehen trotzdem neue Risiken. Sicherheitsstrategien und-kontrollen werden aber in diesem neuen Umfeld nicht automatisch durchgeführt, was sensible Kundendaten einer Gefahr aussetzt. Jeden Tag verstoßen Angestellte gegen unternehmerische Datensicherheit, indem sie öffentliche Cloud-Anwendungen benutzen. Die Unternehmen laufen dadurch Gefahr, gegen Datensicherheit und deren Einhaltung zu verstoßen. Den Cloud-Anbietern mangelt es dann oft an Transparenz in Bezug auf ihre Leistungen, Sicherheit, Datenhoheit und Rückgewinnung. Zudem versäumen es die Unternehmen, ihre Krisenintervention dieser komplizierten Umgebung anzupassen, bei der die Auswirkungen auf das Geschäft nicht vorhersehbar sind.

Was Mazars für Sie tun kann

Mazars unterstützt Sie beim Übergang zum Cloud-basierten IT-System, so dass die Cyber-Sicherheit nicht beeinträchtigt wird und kein Risiko für das Unternehmen entsteht.

UNSERE LÖSUNG BEINHALTET:

- → Unterstützung beim Auswahlprozess im Rahmen der „Cloud first"-Strategie
- → Risikobewertung des Vertrags mit den Cloud-Anbietern nach geschäftlichen und sicherheitsrelevanten Kriterien
- → Analyse und Entwicklung von Strategien und Verfahren
- → Bereitstellung einer unabhängigen Sicherheitsbewertung des Cloud-Anbieters sowie Anpassung an anerkannte Normen und Praktiken wie zum Beispiel ISO 27001, NIST und CSA CCM.
- → Bewertung vom Datenschutz durch Folgenabschätzung und Analyse bei Regelauslassungen hinausgehen.

CYBER ESSENTIALS UND CYBER ESSENTIALS PLUS

Was Mazars für Sie tun kann

Mazars' Sicherheitsexperten unterstützen Sie bei der erfolgreichen Zertifizierung Ihres Unternehmens mit IASME Gold, Cyber Essentials (CE) und Cyber Essentials Plus (CE+).

Diesbezüglich bieten wir zwei Dienstleistungen an:

→ Bereitschaft: Sind Sie bereit für Cyber-Sicherheit? Wir nutzen bei der Übung die gleiche Methodik und Struktur wie während der Prüfung. Die Cybersicherheit wird nicht nur anhand der fünf Bereiche von CE und CE+, sondern auch in Bezug auf die optimale Vorgehensweise bewertet. Wir erstellen einen ausführlichen Bericht mit praktischen Empfehlungen für eine erfolgreiche Zertifizierung. Zusätzlich machen wir Vorschläge, wie eine erstklassige Cyber-Sicherheit zu realisieren ist

→ Zertifizierung: Als offizieller Gutachter für IASME, CE und CE+ kann Mazars bestätigen, dass das Unternehmen mit den Anforderungen konform ist.

Vor dem Hintergrund der zunehmenden Cyber-Bedrohungen und der zahlreichen Sicherheitsverletzungen der letzten Jahre haben die Regierung des Vereinigten Königreichs und die gemeinnützige Organisation „Cyber Streetwise" einen Leitfaden veröffentlicht: Wie können sich Unternehmen im Cyberpace schützen?

CYBER ESSENTIAL UND CYBER ESSENTIALS PLUS

Seit Oktober 2014 müssen Unternehmen den Cyber Essential Kontrollen folgen, wenn sie sich an Ausschreibungen für Regierungsaufträge mit sensiblen bzw. persönlichen Daten beteiligen. Dieses Schema soll kleine und mittlere Unternehmen darin bestärken, die bewährten Verfahren der Informationssicherheit einzuhalten. Während Cyber Essential die Grundlage bildet, bietet Cyber Essential Plus eine höhere Absicherung. Diese ist in fünf Bereiche untergliedert:

1. Boundary Firewalls und Internet Gateways
2. Sichere Konfiguration
3. Nutzer Zugangskontrolle
4. Schutz vor Schadprogrammen
5. Patch Management

ZERTIFIZIERUNG IASME GOLD

Der IASME-Standard (2015 erstmals herausgegeben und im Mai 2015 überarbeitet) wurde eingeführt, um einheitliche Maßstäbe bei der Cyber-Sicherheit für kleine und mittlere Unternehmen zu schaffen. Dieser Standard orientierte sich an den gleichen Grundsätzen wie ISO27001 und NIST 800. Der Standard IASME Gold zeigt eine grundlegende Übereinstimmung mit ISO27001. Diese Norm ergänzt die Cyber Essentials Domain mit den Themen Risikomanagement, Governance, Schulungen, Verfahren, Risikomanagement und Geschäftskontinuität. Ein Unternehmen mit IASME Gold-Zertifikat erhält automatisch auch die Cyber Essential Zertifikation. So können kleine und mittlere Unternehmen mit der praxisnahen und bezahlbaren IASME Auszeichnung beweisen, dass sie sich dem Komplex Informationssicherheit bestmöglich annehmen.

IST IHR UNTERNEHMEN GEGEN EINE SICHERHEITSVERLETZUNG GESCHÜTZT?

Was Mazars für Sie tun kann

Mazars hilft bei der Vorbereitung auf einen Sicherheitsvorfall durch

→ Unabhängige Bewertung, ob bzw. wie gut ein Unternehmen auf einen Cyber-Verstoß vorbereitet ist; erfolgt auf Basis eines Penetrationstestes, Strategien, Verfahren und Kontrollprüfungen

→ Gemeinsame Entwicklung und Implementierung eines Krisenplans

→ Unterstützung während der Testphase

Vor kurzem erließ die US-amerikanische Federal Communication Commission (FCC) eine Strafe gegen den Telekommunikations- und Fernsehanbieter Cox Communication, da er die Datensicherheit nicht ernst nahm und keine Cyber-Krisenintervention vorweisen konnte. Die allgemeine Einschätzung bewegt sich von einem „falls überhaupt eine Cyberattacke das Unternehmen treffen wird" zu einem „wann es wohl soweit sein wird".

Vorbereitung und Planung sind wichtiger denn je. Im Fall eines Sicherheitsverstoßes ist Geschwindigkeit der entscheidende Faktor. Unternehmen müssen gut vorbereitet sein, um schnell reagieren zu können. Nur so kann größerer Schaden, sei es finanzieller oder auch rufschädigender Art, angewendet werden. Die meisten Pläne zur Krisenintervention weisen Defizite auf.

Alle Organisationen sollten einen Cyber-Kriseninterventionsplan implementieren und weiter pflegen, um Schaden abzuwenden und um das Vertrauen der externen Beteiligten (Investoren, Kunden, Regulierungsbehörden) zu stärken. Und auch um Zeit und Geld bei der Wiederherstellung zu sparen.

WARUM MAZARS?

1

STEUERLICHE FACHWISSEN VON EXPERTEN
Mazars hat erstklassige Mitarbeiter und modernste Beratungsdienste im Bereich Cyber-Sicherheit – damit Sie als Kunde ihre Unternehmens-strategie besser umsetzen können.

2

EIN HOCHQUALIFIZIERTES TEAM
Unser team besteht aus versierten Fachkräften, die sich auszeichnen durch professionelle und neutrale Zertifikationen wie CISSP, GPEN, CISA, CRISC, CISM, ISO 27001, CEH und Sie auf Grundlage ihrer Spezialgebiete Technologie, Ingenieurswesen und Computerwissenschaften beraten können.

3

INTERNATIONAL AUFGESTELLT
Das UK Cyber-Team ist Teil von Mazars' internationaler Cyber Security Group mit Exzellenz-Zentren weltweit.

4

STARKE UND WEITREICHENDE ANALYSEN
Dieses Team weiß, wie eine komplexe Umwelt und Projekte zu behandeln sind.

5

VON EINEM ERFAHRENEM TEAM BETREUT
Partner und Senior Manager sind wesentlich in Ihre Beratung involviert.

6

EIN MASSGESCHNEIDERTER ANSATZ
Wir konzipieren individuelle Dienstleistungen für jeden Kunden. Das ist Maßarbeit für Sie!

7

LÖSUNGSORIENTIERT
Wir erarbeiten Lösungen für Sie, die praxisnah und pragmatisch sind.

8

WIR VERTRETEN WERTE
Sie bekommen höchste Dienstleistungsqualität zu fairen Preisen.

9

ANSPRECHBAR UND ERREICHBAR
Wir wollen für Sie erreichbar sein. Das hat oberste Priorität.

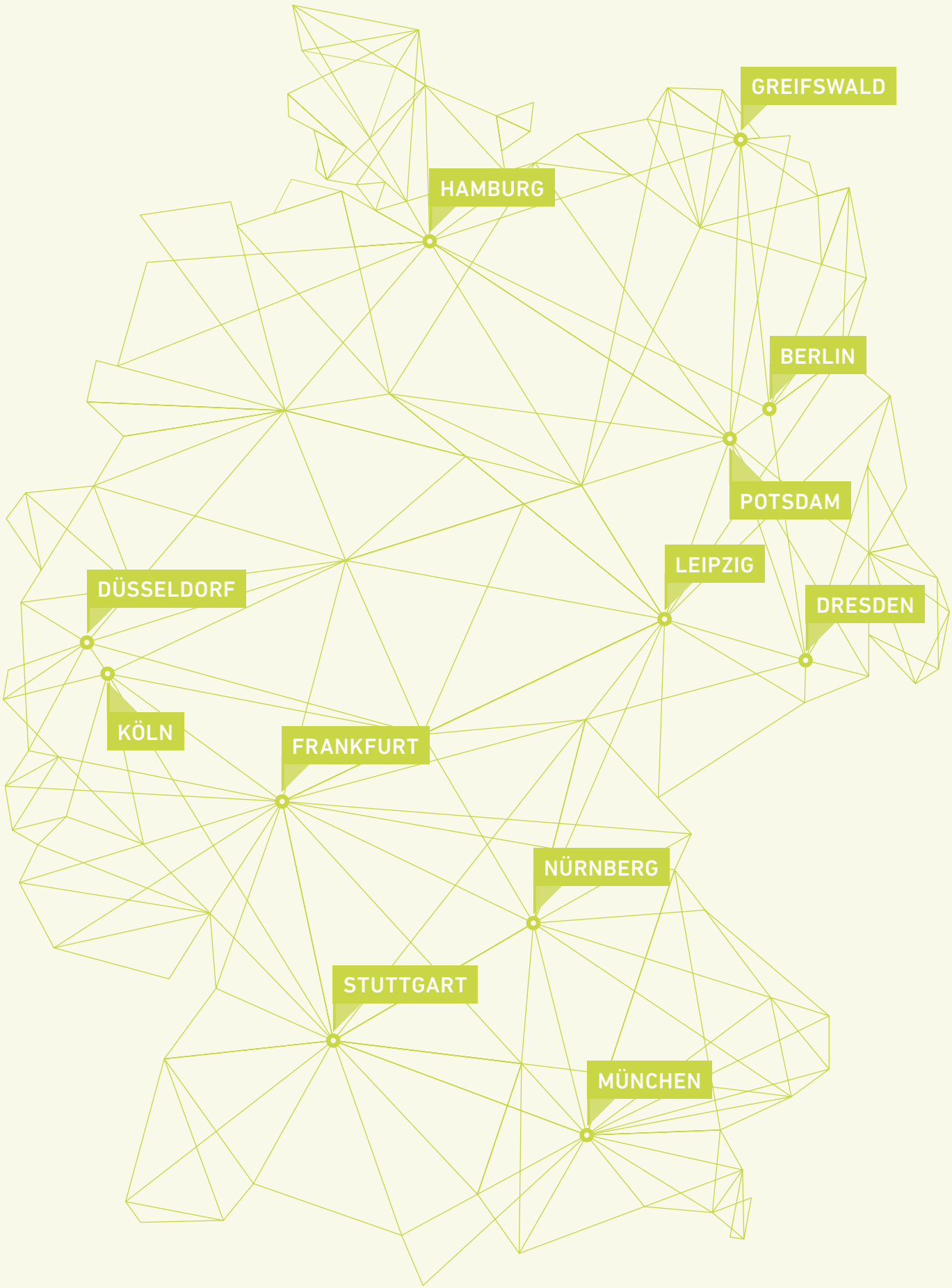
ANSPRECHPARTNER

Stefan Wittjen
CISA, CIA, CISM, CRISC,
QA, QAR-IT
Senior Manager

Tel: +49 30 208 88-1170
stefan.wittjen@mazars.de

Andreas Janoschek
Manager

Tel: +49 30 208 88-1150
andreas.janoschek@mazars.de


GREIFSWALD
HAMBURG
BERLIN
POTSDAM
LEIPZIG
DÜSSELDORF
DRESDEN
KÖLN
FRANKFURT
NÜRNBERG
STUTTGART
MÜNCHEN

STANDORTE

Berlin
Alt-Moabit 2
10557 Berlin
Tel: +49 30 208 88-0

Dresden
Kleine Brüdergasse 3
01067 Dresden
Tel: +49 351 45 15-0

Düsseldorf
Bennigsen-Platz 1
40474 Düsseldorf
Tel: +49 211 83 99-0

Frankfurt am Main
Theodor-Stern-Kai 1
60596 Frankfurt am Main
Tel: +49 69 967 65-0

Greifswald
Steinbeckerstraße 10
17489 Greifswald
Tel: +49 3834 885 33-40

Hamburg
Domstraße 15
20095 Hamburg
Tel: +49 40 288 01-0

Köln
Gustav-Heinemann-Ufer 72
50968 Köln
Tel: +49 221 28 20-0

Leipzig
Petersstraße 1–13
04109 Leipzig
Tel: +49 341 60 03-0

München
Herzog-Heinrich-Straße 22
80336 München
Tel: +49 89 350 00-0

Nürnberg
Längenstraße 14
90491 Nürnberg
Tel: +49 911 60 07-0

Potsdam
Hebbelstraße 27
14469 Potsdam
Tel: +49 331 73 04 07-70

Stuttgart
Friedrichstraße 10
70174 Stuttgart
Tel: +49 711 60 17 87-0

DE 12/2016

Roever Broenner Susat Mazars
GmbH & Co. KG
Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft
Domstraße 15
20095 Hamburg

www.mazars.de