NORTHWAVE
CYBER SECURITY

Global Threat Landscape 2026

Strategisch führen mit Threat Intelligence

Aktuelle Cyberbedrohungen auf einen Blick

Eine Entwicklung sticht im Jahr 2026 besonders hervor: Cyberrisiken bewegen sich inzwischen mit maschineller Geschwindigkeit. Künstliche Intelligenz verschiebt das Gleichgewicht zwischen Angreifern und Verteidigern – wobei die Verteidiger zunehmend ins Hintertreffen geraten.

Bedrohungsakteure sind schneller und anpassungsfähiger als je zuvor. Exploits werden inzwischen in großem Maße automatisiert. Angriffe basieren zunehmend sowohl auf Identitätsdaten als auch auf Sicherheitslücken, da Angreifer die Vertrauensbeziehungen, auf die moderne Unternehmen angewiesen sind, systematisch missbrauchen.

Wichtige Entwicklungen, die wir beobachten:

- KI ermöglicht es Angreifern zunehmend, schneller zu agieren, als Organisationen analysieren, patchen und reagieren können
- Identitäten und Schwachstellen werden zu parallelen Zugangspfaden
- Vertrauen wird in großem Maßstab ausgenutzt
- Cyberkriminalität, Spionage, Sabotage und Einflussnahme wachsen zusammen
- Die Auswirkungen verlagern sich hin zu Daten-, rechtlichen und strategischen Risiken

43 Tage Medianzeit, bis eine Organisation einen Patch nach Verfügbarkeit installiert

Angriffe erfolgen im Schnitt **7 Tage** vor Bereitstellung eines Patches

Wie sich Ihr Risiko verschiebt

Von → Zu

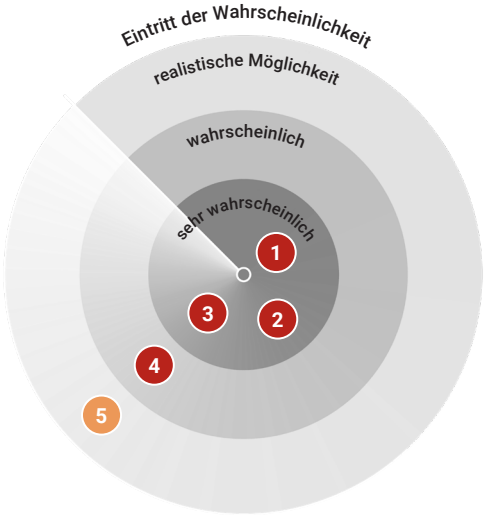
- Systeme → Identitäten
- Einzelvorfälle → Persistente Zugriffe
- Störungen → Daten- und regulatorische Risiken
- IT-Risiken → Geschäftsrisiken
- Isolierte Angriffe → Strategische Konsequenzen

Top 5 Cyberrisiken mit Priorität

Die konkrete Rangfolge unterscheidet sich je nach Branche und Organisationsstruktur.

1. **Cyber-Erpressung** (Cyber Extortion)
   - Daten als Druckmittel.
2. **Business Email Compromise** (BEC)
   - Identitätsmissbrauch im großen Maßstab.
3. **Insider-Bedrohungen** (Insider Threats)
   - Datenzugriff ohne ausreichende Kontrolle
4. **Staatlich gelenkte Cyberangriffe** (Nation-State Attacks)
   - Dauerhaftes Eindringen, Datenoffenlegung und Störung
5. **Staatlich unterstützter Hacktivismus** (State-Aligned Hacktivism)
   - Sabotage und Desinformation.

Unser **Threat Radar** visualisiert die Wahrscheinlichkeit und die Auswirkungen von Bedrohungen.



Definition der Bedrohungsauswirkungen (Impact)

- **Gering (Low):** Geringer Reputationsschaden, finanzieller Verlust, rechtliche/regulatorische Konsequenzen und/oder Beeinträchtigungen des Geschäftsbetriebs. **Keine zusätzlichen Maßnahmen erforderlich.**
- **Mittel (Medium):** Signifikanter Reputationsschaden, finanzieller Verlust, rechtliche/regulatorische Konsequenzen und/oder Betriebsunterbrechung. **Maßnahmen ergreifen, wenn die Kosten-Nutzen-Analyse signifikant ist.**
- **Hoch (High):** (Sehr) schwerer Reputationsschaden, finanzieller Verlust, rechtliche/regulatorische Konsequenzen und/oder Betriebsunterbrechung. **Mit höchster Priorität eindämmen und Maßnahmen ergreifen, bis das Risiko auf ein akzeptables Maß reduziert ist.**

Auf den folgenden Seiten erfahren Sie mehr darüber, was diese Bedrohungen heute für europäische Unternehmen bedeuten und welche Abwehrstrategien wir empfehlen. Wie immer plädieren wir für einen ganzheitlichen Ansatz, der die geschäftlichen (**business**), technischen (**bytes**) und verhaltensbezogenen (**behavioural**) Aspekte der Cybersicherheit abdeckt.

Cyber-Erpressung
(Cyber Extortion)

„Nicht Systemausfälle treiben heute den Impact – sondern Datenexponierung und regulatorische Haftung.“

Ransomware zielte ursprünglich darauf ab, Systeme zu verschlüsseln. Heute priorisieren moderne Cyber-Erpressungstaktiken jedoch zunehmend die Exfiltration von Daten – ergänzend oder anstelle von Verschlüsselung. Angreifer nutzen die Androhung von Veröffentlichung, um den Druck zu erhöhen. Dadurch übersteigen Reputationsschäden, rechtliche Risiken und regulatorische Konsequenzen häufig die Auswirkungen von Betriebsunterbrechungen.

Mehr als 8.000 Organisationen weltweit wurden im Jahr 2025 auf Leak-Seiten veröffentlicht. Im Jahr 2026 beobachten wir zudem den Einsatz von KI zur Beschleunigung von Angriffen, wodurch Organisationen nur noch ein sehr begrenztes Zeitfenster für Erkennung, Eindämmung und Reaktion bleibt. Die Herausforderung besteht damit nicht mehr nur in der Wiederherstellung, sondern vor allem in der Kontrolle von Datenexposition und der schnellen Entscheidungsfindung unter hohem Druck.

Wichtige Verteidigungsstrategien

Eine effektive Abwehr von Cyber-Erpressung erfordert frühzeitige Erkennung, das Einschränken und Verlangsamen von Angreiferbewegungen, die Reduzierung von Druckmitteln sowie schnelle Entscheidungsfähigkeit unter Druck – begleitet von klarer Krisenkommunikation.

- Etablieren Sie eine klare Krisen-Governance über Incident Response, Recht und Kommunikation hinweg.
- Führen Sie funktionsübergreifende Krisensimulationen durch, damit Reaktionen auch unter Druck zur Routine werden.
- Richten Sie Ihre Reaktionsprozesse frühzeitig an regulatorischen Anforderungen aus (z.B. DSGVO, NIS2).

- Implementieren Sie MDR/SOC mit frühzeitiger Erkennung über Identität, Cloud und Netzwerk hinweg – nicht nur auf Endpoint-Ebene.
- Überwachen Sie Datenexfiltration, Manipulation von Backups sowie Verschlüsselungsaktivitäten als prioritäre Frühindikatoren.
- Setzen Sie grundlegende Sicherheitsmaßnahmen konsequent um: Offline-Backups, phishing-resistente MFA und Netzwerksegmentierung.

- Schulen Sie Mitarbeitende darin, fortgeschrittene Social-Engineering-Techniken und MFA-Umgehungsmethoden zu erkennen.
- Stärken Sie kritische Verhaltensweisen wie das Melden verdächtiger Aktivitäten und den sicheren Umgang mit Daten.
- Setzen Sie auf szenariobasiertes Training, das sich an realen Angriffsmustern orientiert.

Business Email Compromise (BEC)

„Wo einer Identität vertraut wird, wird Malware überflüssig für Angreifer.“

2025 entfielen über 40 % der Northwave Incident-Response-Fälle auf BEC – mehr als auf Cyber-Erpressung. Angreifer weichen zunehmend auf Session-Diebstahl und identitätsbasierte Angriffe aus, die traditionelle Schutzmaßnahmen wie MFA umgehen.

Die Bedrohung weitet sich branchenübergreifend aus – besonders betroffen sind Industrie sowie Business Services, vor allem die Rechtsbranche. Phishing wird überzeugender und skalierbarer, individuell angepasst an Sprache und Kontext. In Kombination mit KI-gestütztem Social Engineering erhöht sich das Risiko von Betrug und Datenverlust deutlich.

Wichtige Verteidigungsstrategien

Stärken Sie Identitäten und Geschäftsprozesse, um BEC-Risiken zu minimieren. Unterbinden Sie technische Angriffspfade und verlassen Sie sich nicht ausschließlich auf menschliches Vertrauen.

- Führen Sie strikte Prüfprozesse für Zahlungen ein, insbesondere bei Änderungen von Bankverbindungen und dringenden Überweisungen.
- Wenden Sie das Vier-Augen-Prinzip bei risikoreichen Transaktionen und sensiblen Vorgängen an.
- Definieren Sie klare Freigabeprozesse sowie Eskalationswege für finanzielle und zugriffsbezogene Anfragen.

- Integrieren Sie phishing-resistente MFA und Conditional Access in Ihre Identitäts-Baseline.
- Erkennen und unterbinden Sie den Missbrauch von OAuth sowie Manipulationen an Postfächern (z. B. Weiterleitungen und Regeländerungen).
- Stellen Sie eine starke E-Mail-Sicherheit sicher (SPF, DKIM, DMARC, Anti-Spoofing, erweiterte Filtermechanismen).

- Schulen Sie Mitarbeitende darin, risikoreiche Anfragen zu Zahlungen oder Zugangsdaten sorgfältig zu überprüfen.
- Fördern Sie eine Kultur, in der Innehalten und Prüfen „Stop & Check!“ ausdrücklich erwartet wird.
- Schulen Sie im Umgang mit kanalübergreifendem Social Engineering (E-Mail, Telefon, Video) und ermöglichen Sie eine einfache Meldung verdächtiger Vorfälle.

Insider-Bedrohungen
(Insider Threats)

„Insider-Risiken entstehen durch fehlende Kontrolle über Zugriffe, nicht durch böse Absichten.“

Die meisten Insider-Vorfälle betreffen Mitarbeitende, Auftragnehmer, Dritte – und zunehmend auch KI-Agenten. Sie entstehen in der Regel durch Fehler, Fahrlässigkeit oder fehlende Kontrolle und nicht durch böswillige Absicht. Rund ein Drittel der Datenpannen in Europa ist darauf zurückzuführen, besonders häufig in großen Organisationen, in denen Komplexität und Mitarbeiterfluktuation die Angriffsfläche erhöhen.

Die zunehmende Nutzung von Cloud-, SaaS- und KI-Tools – einschließlich autonomer Agenten – hat dieses Risiko deutlich verstärkt, da sie einen schnellen Zugriff auf sensible Daten und deren Bewegung ermöglichen. Gleichzeitig nehmen KI-bedingte Datenlecks in Organisationen zu, oft bedingt durch fehlende Schulung, unzureichende Governance und mangelnde Transparenz darüber, wie Daten verwendet werden.

Wichtige Verteidigungsstrategien

Reduzieren Sie Insider-Risiken durch kontrollierten Zugriff, Verhaltensüberwachung und indem Sie Mitarbeitende befähigen, standardmäßig sichere Entscheidungen zu treffen.

- Implementieren Sie strukturierte Onboarding- und Offboarding-Prozesse, einschließlich der rechtzeitigen Vergabe und Entziehung von Zugriffsrechten.
- Definieren und durchsetzen klarer Richtlinien für zulässige Nutzung und fahrlässiges Verhalten.
- Fördern Sie eine offene Meldekultur mit klaren Eskalationswegen und Whistleblowing-Mechanismen.

- Setzen Sie das Least-Privilege-Prinzip durch und verlangen Sie verwaltete, vertrauenswürdige Geräte für den Zugriff auf sensible Daten.
- Implementieren Sie Datenklassifizierung und DLP, um den Umgang mit sensiblen Daten zu überwachen und einzuschränken.
- Stellen Sie Transparenz über Nutzeraktivitäten und nicht autorisierte Tools sicher, einschließlich der Kontrolle über KI-Systeme und externe Integrationen.

- Bieten Sie kontinuierliche, praxisnahe Schulungen mit Fokus auf reale Bedrohungen und KI-bezogene Risiken.
- Stärken Sie sichere Alltagsverhaltensweisen im Umgang mit sensiblen Daten.
- Schaffen Sie eine Unternehmenskultur, in der Mitarbeitende Fehler offen melden und unklare Situationen hinterfragen können.

Staatlich gelenkte Cyberangriffe (Nation-State Attacks)

„Verdeckt, langfristig und gezielt darauf ausgelegt, der Erkennung zu entgehen.“

Nationalstaatliche Cyberaktivitäten betreffen inzwischen nahezu alle großen europäischen Branchen – von Verteidigung und Energie über Industrie und Logistik bis hin zu den Life Sciences. Nahezu alle EU-Länder sind betroffen, wobei Deutschland, Polen und Frankreich besonders exponiert sind. Diese Angriffe werden in der Regel von sogenannten Advanced Persistent Threats (APTs) durchgeführt – gut ausgestatteten, staatlich unterstützten Kampagnen oder deren Stellvertretern, die auf Unternehmensnetzwerke, Lieferketten und geistiges Eigentum abzielen.

Für Organisationen stellt dies ein dauerhaftes Geschäftsrisiko dar. Angreifer kombinieren Identitätsmissbrauch, Social Engineering, Insider-Methoden sowie die Ausnutzung von Cloud- und Edge-Umgebungen. Diese Angriffe sind darauf ausgelegt, unentdeckt zu bleiben, über lange Zeiträume zu operieren und strategische Auswirkungen zu erzielen. China betreibt in Europa eine anhaltende und groß angelegte Datensammlung, während Russland aktiv Sabotageversuche durchführt.

Wichtige Verteidigungsstrategien

Schützen Sie sich vor persistierenden Angriffen, indem Sie die Erkennung beschleunigen, gezielt Reibung für Angreifer schaffen und sich auf eine langfristige, intelligence-getriebene Reaktion vorbereiten.

- Behandeln Sie Identitäten, Cloud-Plattformen und Edge-Umgebungen als Tier 1-Risikobereiche – mit klarer Verantwortung und Governance.
- Beziehen Sie Lieferketten und Drittparteien als Teil Ihrer internen Angriffsfläche ein, mit verbindlichen Sicherheitsanforderungen und regelmäßigen Überprüfungen.
- Bereiten Sie Führungskräfte durch Angreifersimulationen und Krisenübungen darauf vor, unter Unsicherheit und in langanhaltenden Bedrohungsszenarien handlungsfähig zu bleiben.

- Setzen Sie phishing-resistente MFA und risikobasierten Conditional Access für kritische Nutzer und Systeme konsequent durch.
- Verlagern Sie die Erkennung hin zu verhaltensbasiertem Monitoring und TTP-Analysen über Identität, Cloud, Endpoint und Netzwerk hinweg.
- Reduzieren Sie die Angriffsfläche durch Härtung von Endpoints und Edge-Systemen sowie durch sichere Baseline-Konfigurationen.

- Bieten Sie rollenbasierte Schulungen für besonders risikoreiche und privilegierte Nutzer an, mit Fokus auf gezieltes Social Engineering.
- Bereiten Sie Mitarbeitende und Krisenteams auf APT-Szenarien und langanhaltende Vorfälle vor.
- Stärken Sie die Reaktionsfähigkeit, damit Entscheidungsfindung und Koordination auch unter Druck effektiv bleiben.

Staatsnaher Aktivismus (State-Aligned Hacktivism)

„Das Risiko wird weniger durch technische Raffinesse bestimmt, sondern vielmehr durch Skalierung, Sichtbarkeit und Timing.“

Hacktivismus stellt weiterhin eine anhaltende Bedrohung für europäische Organisationen dar und ist heute überwiegend staatlich geprägt. Seit Beginn des Krieges in der Ukraine haben pro-russische Gruppen kontinuierliche DDoS-Kampagnen gegen Behörden, Finanzwesen, Einzelhandel, Medien, Logistik und Technologie durchgeführt. Einzelne Vorfälle haben oft nur begrenzte Auswirkungen, doch ihre Häufigkeit erzeugt anhaltenden operativen Druck – insbesondere in politisch sensiblen Phasen.

Störungen werden häufig mit Desinformation kombiniert, wodurch der Reputationsschaden verstärkt wird, selbst wenn der technische Schaden begrenzt bleibt. Sowohl mutmaßliche als auch bestätigte Eingriffe in industrielle Systeme nehmen zu und schaffen Unsicherheit sowie zusätzlichen Druck. Wenn Hacktivismus OT-Umgebungen in kritischen Sektoren betrifft, kann bereits ein begrenzter Zugriff Abläufe stören, Sicherheitsrisiken verursachen und regulatorische Konsequenzen auslösen.

Wichtige Verteidigungsstrategien

Konzentrieren Sie sich auf Resilienz statt auf reine Prävention. Fangen Sie Störungen ab, bewahren Sie Vertrauen und sichern Sie den Betrieb auch unter anhaltendem Druck.

- Etablieren Sie eine klare Krisen-Governance über Incident Response, Kommunikation und Business Continuity hinweg.
- Bereiten Sie sich darauf vor, schnell und konsistent auf Desinformation und unbestätigte Behauptungen zu reagieren.
- Stellen Sie sicher, dass für kritische Systeme und Services im Störungsfall geeignete Ausweichlösungen verfügbar sind.

- Sichern Sie extern erreichbare Systeme durch konsequentes Patchen, Logging, Monitoring und starke Zugriffskontrollen ab.
- Implementieren Sie Anti-DDoS-Schutz und Web Application Firewalls, um Angriffe auch im großen Maßstab abzuwehren.
- Segmentieren Sie IT- und OT-Umgebungen und beschränken Sie die direkte Internetexposition kritischer Systeme.

- Schulen Sie Krisenteams, auch bei langanhaltenden Störungen handlungsfähig zu bleiben und bereichsübergreifend zwischen Security und Kommunikation zu koordinieren.
- Schärfen Sie das Bewusstsein für Desinformationsrisiken und differenzieren Sie klar zwischen technischem Impact und kommunikativem bzw. narrativem Druck.
- Stärken Sie die Vorbereitung auf eingeschränkte Betriebsfähigkeit und anhaltende Störungen.

Verteidigungsstrategien für das KI-Zeitalter

„Angreifer handeln schneller, als Unternehmen analysieren, patchen und reagieren können.“

Cyberbedrohungen werden durch zugrunde liegende Kräfte – sogenannte Treiber – geprägt, die bestimmen, warum bestimmte Bedrohungen zunehmen, wie schnell sie sich entwickeln und welche Auswirkungen sie haben. Unter den zentralen Treibern, die wir in unserem Global Threat Landscape 2026 identifiziert haben, wirkt keiner so stark als Multiplikator wie Künstliche Intelligenz.

Angreifer nutzen KI heute, um Angriffe deutlich schneller und einfacher zu planen, durchzuführen und zu skalieren. KI verfeinert Social Engineering, beschleunigt die Identifikation und Ausnutzung von Schwachstellen und senkt die Einstiegshürden für Angreifer. Staatliche gelenkte Cyber-Akteure stehen an der Spitze dieser Entwicklung, dicht gefolgt von kriminellen Akteuren.

Der größte Einfluss auf die Cyberabwehr wird von agentenbasierenden, durch KI orchestrierten Angriffen ausgehen. Mit zunehmender Autonomie von KI-Systemen wird sich sowohl die Geschwindigkeit als auch das Volumen von Angriffen deutlich erhöhen. Angriffsmuster werden weniger vorhersehbar, da KI-Unterstützung es Angreifern erleichtert, neue Schwachstellen zu entdecken und sich in Echtzeit an veränderte Bedingungen anzupassen.

Für europäische Organisationen ist dies kein einzelner Wendepunkt, sondern ein kontinuierlich steigender Druck. **Viele Organisationen arbeiten noch mit Annahmen aus der Zeit vor KI, während Angreifer die veränderten Rahmenbedingungen bereits aktiv ausnutzen.**

Was Organisationen jetzt tun müssen

1. Begrenzen, was Angreifer erreichen können

Agentenbasierte, KI orchestrierte Angriffe erhöhen den Druck auf exponierte Systeme, öffentlich zugängliche Schnittstellen, Cloud-Umgebungen und unzureichend gesteuerte Assets. Es ist entscheidend, die eigene externe Angriffsfläche zu kennen und sie, wo möglich, zu reduzieren.

Fokus auf:

- Öffentlich zugängliche Systeme
- Cloud-Services
- Webanwendungen
- Exponierte Schnittstellen
- Netzwerknahe Geräte (Edge Devices)

Alles, was weiterhin exponiert ist, muss kontinuierlich überwacht und schnell gepatcht werden.

2. Angreifer ausbremsen

KI gestützte Angreifer agieren mit Maschinengeschwindigkeit – daher ist es entscheidend, gezielt Hindernisse zu schaffen, um ihren Fortschritt zu verlangsamen. Dazu gehören:

- Netzwerksegmentierung
- Identitätssegmentierung
- Just-in-Time (JIT) für privilegierte Zugriffe
- Gestaffelte Administratorumgebungen
- Starke Zugriffskontrollen für Cloud- und SaaS-Dienste

Diese Maßnahmen entfalten ihren vollen Nutzen jedoch nur, wenn sie mit wirksamen Detektionsmechanismen kombiniert werden.

3. Erkennung und Reaktion beschleunigen

Die Reaktion auf laufende Angriffe muss deutlich schneller erfolgen. Analyse von Alarmen sowie erste aktive Maßnahmen zur Eindämmung sollten daher ebenfalls durch agentenbasierte KI unterstützt werden. Zudem benötigen SOC- und MDR-Funktionen Transparenz über:

- Identitäten
- Cloud-Umgebungen
- Endpoints
- Netzwerk-Edge
- Applikationen
- Privilegien, Accounts, Schlüssel und Tokens

Diese Transparenz liefert die grundlegende Informationsbasis für schnelle und fundierte Entscheidungen. Gleichzeitig fließen alle Erkenntnisse in Ihren Incident-Response-Prozess ein, der weiterhin maßgeblich von Menschen gesteuert wird. Die Abläufe zur Bewältigung von Vorfällen sollten klar definiert sein – in Bezug auf Kommunikation, Verantwortlichkeiten und Prozessschritte. Mitarbeitende sollten regelmäßig und konsistent geschult werden, damit die Reaktion im Ernstfall routiniert und selbstverständlich erfolgt.

So unterstützt Sie Northwave

Im Jahr 2026 ist Cyberrisiko endgültig im Vorstand angekommen – als Thema der Governance und strategischen Steuerung. Die Fähigkeit, schnell und entschlossen zu handeln, war noch nie so entscheidend wie heute.

Unsere Threat Intelligence und Handlungsperspektiven bieten Ihnen einen Ausgangspunkt. Laden Sie den vollständigen Global Threat Landscape Report herunter, um unsere Expertenerkenntnisse im Detail zu entdecken.

Für eine individuelle Beratung sprechen Sie uns an. Gemeinsam übersetzen wir diese Erkenntnisse in gezielte Maßnahmen für Ihre Organisation.

Jetzt scannen und den vollständigen Global Threat Landscape Report 2026 von Northwave lesen!

Über Northwave Cyber Security

Northwave Cyber Security ist ein führender europäischer Spezialist, der Organisationen dabei unterstützt, ihre Resilienz zu stärken und effektiv auf Cybervorfälle zu reagieren. Das Unternehmen wurde 2006 in den Niederlanden gegründet und ist in den Regionen Benelux, DACH und Nordics tätig, mit Standorten in Utrecht (Niederlande), Leipzig (Deutschland), Brüssel (Belgien) und Stockholm (Schweden).

Das Team von Northwave besteht aus über 275 Expertinnen und Experten in den Bereichen IT-Sicherheit, Forensik, Psychologie, Recht, Kriminologie, Cyber Threat Intelligence und Risikomanagement. Die integrierten Lösungen verbinden Technologie, Prozesse und Erkenntnisse zu menschlichem Verhalten zu einem ganzheitlichen Sicherheitsansatz.

Seit 2012 unterstützt das zertifizierte Computer Emergency Response Team von Northwave (NW CERT) Unternehmen weltweit bei der Reaktion auf und der Wiederherstellung nach Ransomware-Angriffen, Datenpannen und anderen Sicherheitsvorfällen.

Weitere Informationen finden Sie unter: **northwave-cybersecurity.com**

24/7 Computer Emergency Response Team
+49 (0)341 2387 0004

NORTHWAVE
CYBER SECURITY

Northwave Deutschland GmbH
+49 341 33 977 898
dach@northwave-cybersecurity.com
Alte Messe 1a, 04103 Leipzig, Deutschland
Sitz der Gesellschaft: Leipzig
Registergericht: Amtsgericht Leipzig, HRB 37746
Umsatzsteuer-ID: DE 332197502