



Betrugsnetzwerke erkennen: Linkanalyse mit InfoZoom

Jennifer Kambeck
corma GmbH

Über uns

Unternehmensgründung: 1999

- Geschäftsbereich: professionelle Ermittlungen für weltweite Aufklärung von Wirtschafts- und Betrugsdelikten, Produkt- und Markenpiraterie
- Firmensitz Deutschland, weltweite Einsätze für Kunden lokalisiert in Europa und den Vereinigten Staaten (Referenzen gerne auf Anfrage)
- Kern-Team: zertifizierte Ermittler, Analysten (IZCP), Certified Fraud Examiners (CFE)

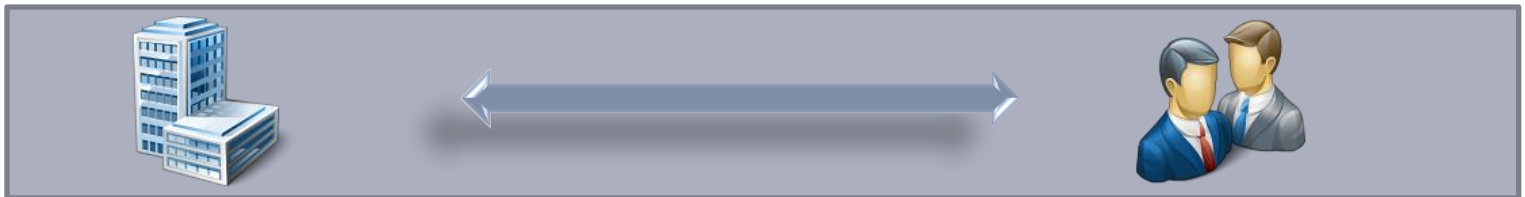


Dienstleistungen



Kundenprofil

**Global operierender IT Hersteller oder
Jedes Unternehmen mit angebotenen Garantiedienstleistungen**

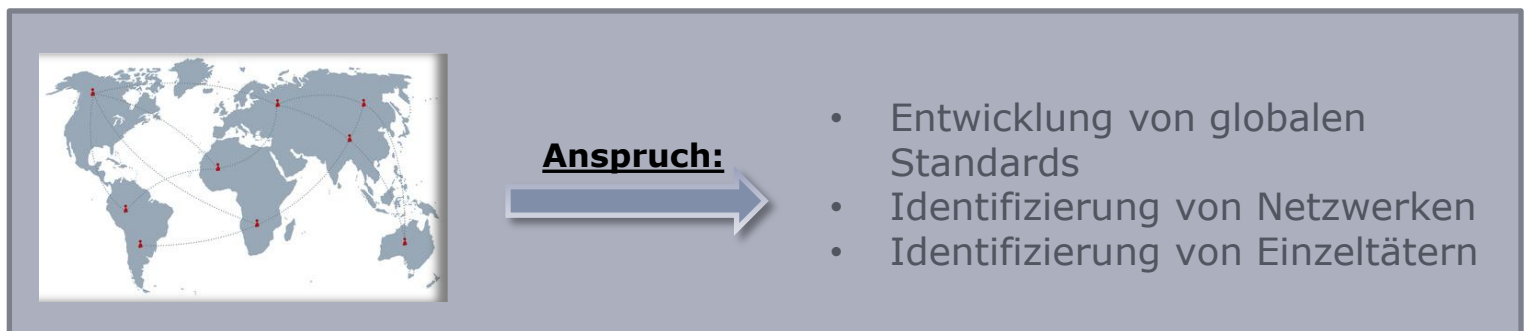


Verluste durch Ausnutzung der Garantieb Bestimmungen durch:

- Endkunden
- Partner
- Mitarbeiter

Analysen und Ermittlungen in:

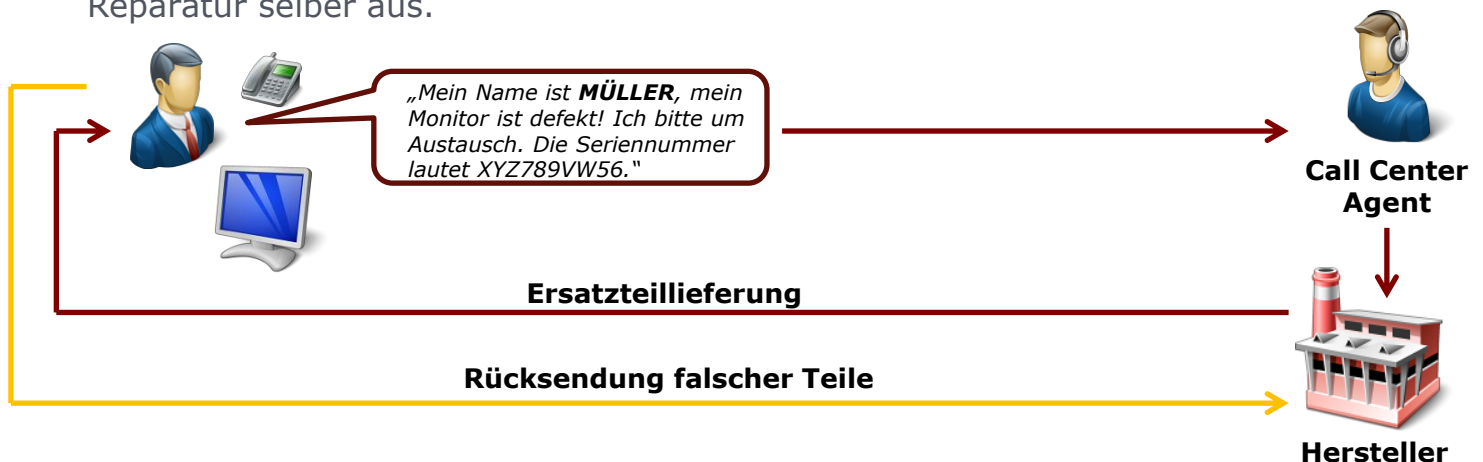
- Teams weltweit
- Verschiedenen Datenquellen
- Unterschiedliche Analyseansätze



- Entwicklung von globalen Standards
- Identifizierung von Netzwerken
- Identifizierung von Einzeltätern

Fallbeispiel

- Ein IT Hersteller bietet für definierte Garantiefälle einen sogenannten Selbstaustausch an.
- In diesem Fall wird dem Endkunden das Ersatzteil zugesandt und dieser führt die Reparatur selber aus.



- Im Anschluss wird das defekte Gerät an den Hersteller zurückgeschickt.
- In unserem Fall hat der Hersteller Häufungen an Rücksendungen mit falschen oder manipulierten Teilen festgestellt und bittet um Prüfung der Falldaten zu den betroffenen Garantiefällen.
- Die gelieferten Rohdaten werden in für dieses Szenario entworfene InfoZoom Templates geladen und analysiert.

Vorlagen, Vorlagen, Vorlagen!

Kontinuierliche Analyse der Garantiedaten erfordert:

- Definierte Struktur der Rohdaten
- Standardisierte Aufbereitung dieser Daten
- Einheitliche Analysegrundlagen als Basis für jede Ermittlung

Entwicklung und konsequenter Einsatz von Vorlagen

- Massive Zeiteinsparung
- „ready to use“ durch klare, vordefinierte Dateistruktur
- Ergebnisse flaggen
- Analyseergebnis ist für jedes Teammitglied sofort ersichtlich

| 118 Attribute | |
|---------------|----------------------|
| ▼ | Kennung |
| ▼ | UniqueID |
| + | Garantiefall |
| + | Fallerstellung |
| + | Kunde |
| + | Produkt |
| + | Teil |
| + | Lieferdaten |
| + | #### ANALYSE #### |
| + | #### ERGEBNISSE #### |

Netzwerke erkennen

Überprüfung „Anzahl von“:

Gibt es mehrere Kunden...

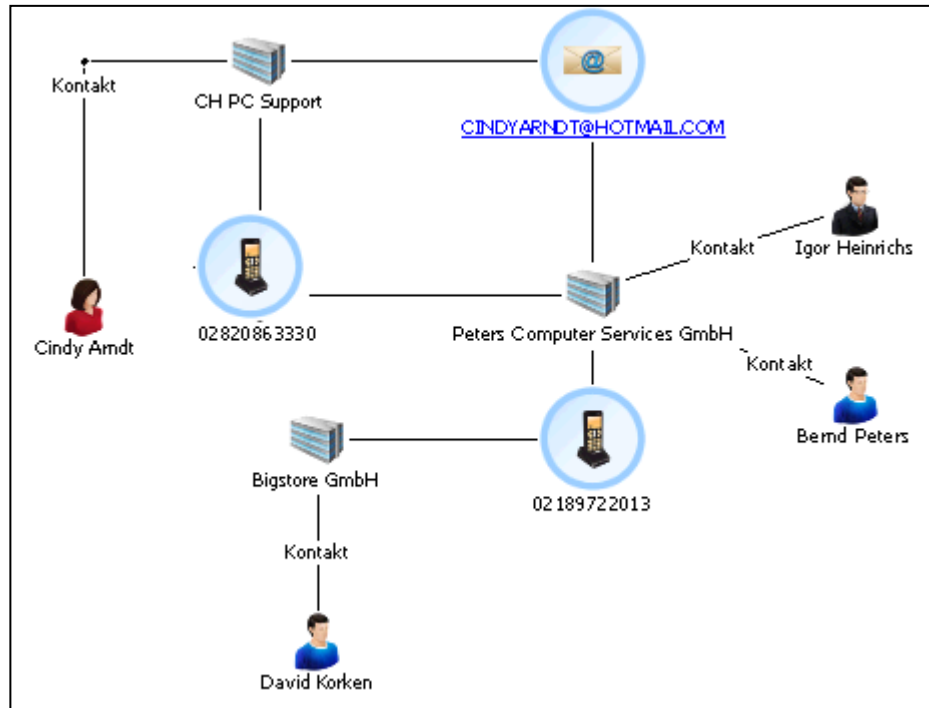
- für die gleiche Seriennummer?
- mit der gleichen Telefonnummer?
- an der gleichen Adresse?

Beispiel: Verschiedene Kunden pro Seriennummer



| | | |
|--------------------------------|--------|------|
| 2. Verschiedene Kunden pro SN | | |
| Analyseergebnis | prüfen | okay |
| Verschiedene Kunden pro SN | | |
| Seriennummer | | |
| Produkt | | |
| Anzahl(Kunde) | 2 | 1 |
| 2.1 Überblick | | |
| Anzahl Kunden | 2 | 1 |
| Anzahl Seriennummern pro Kunde | 16 | 643 |

Erstes Ergebnis:



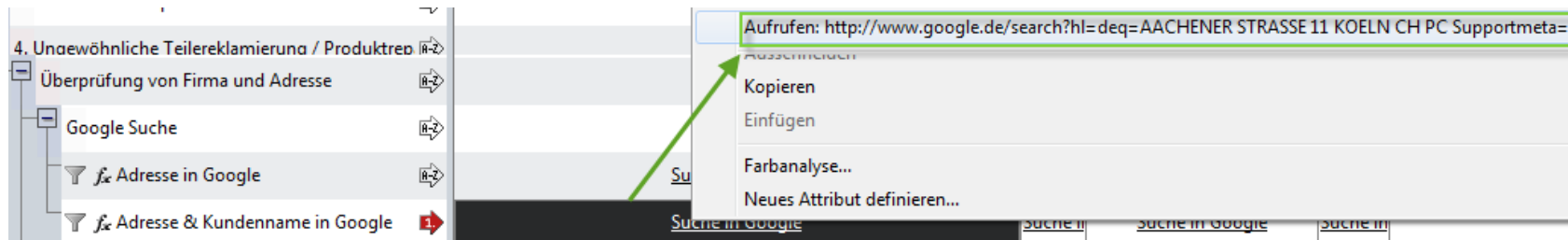
**Alle Firmen
geben
verschiedene
Adressen an!**

iResearch via InfoZoom (1)

Validierung via Googlemaps & Googlesuche für

- Kundenadresse
- Firmenname & Adresse

 → *nur 1 Firma konnte mit der angegebenen Adresse verifiziert werden*

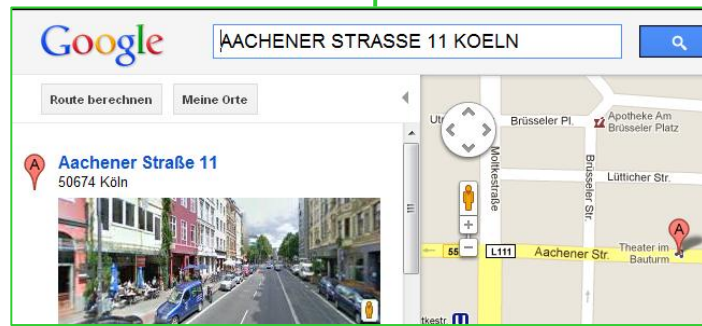


The screenshot shows a software interface with a list of search steps on the left and a context menu on the right. The steps are:

- 4. Unauwöhnliche Teilereklamierung / Produktred
- Überprüfung von Firma und Adresse
- Google Suche
- Adresse in Google
- Adresse & Kundenname in Google

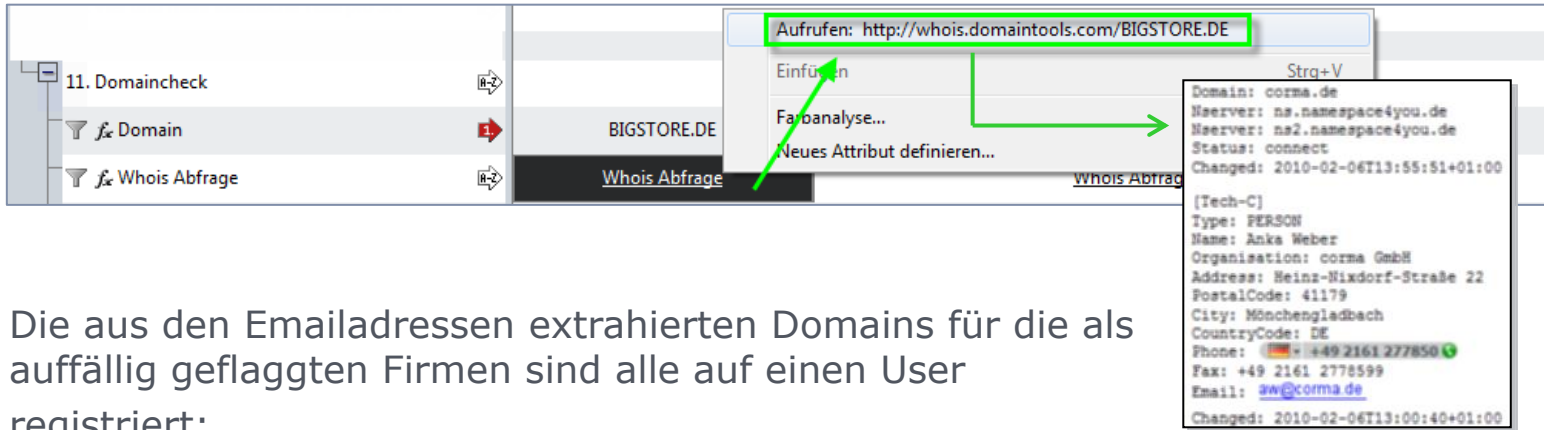
The context menu is open over the 'Suche in Google' step, showing the following options:

- Aufrufen: <http://www.google.de/search?hl=de&q=AACHENER STRASSE 11 KOELN CH PC Supportmeta=>
- Ausschneiden
- Kopieren
- Einfügen
- Farbanalyse...
- Neues Attribut definieren...



iResearch via InfoZoom (2)

Domaincheck via InfoZoom Formel



11. Domaincheck

- Domain
- Whois Abfrage

BIGSTORE.DE

Whois Abfrage

Aufrufen: <http://whois.domaintools.com/BIGSTORE.DE>

Einfügen

Feldanalyse...

Neues Attribut definieren...

Strg+V

Domain: corma.de
Nservers: ns.namespace4you.de
Nservers: ns2.namespace4you.de
Status: connect
Changed: 2010-02-06T13:55:51+01:00

[Tech-C]
Type: PERSON
Name: Anka Weber
Organisation: corma GmbH
Address: Heinz-Nixdorf-Straße 22
PostalCode: 41179
City: Mönchengladbach
CountryCode: DE
Phone: +49 2161 277850
Fax: +49 2161 2778599
Email: aw@corma.de
Changed: 2010-02-06T13:00:40+01:00

Die aus den Emailadressen extrahierten Domains für die als auffällig geflaggtten Firmen sind alle auf einen User registriert:

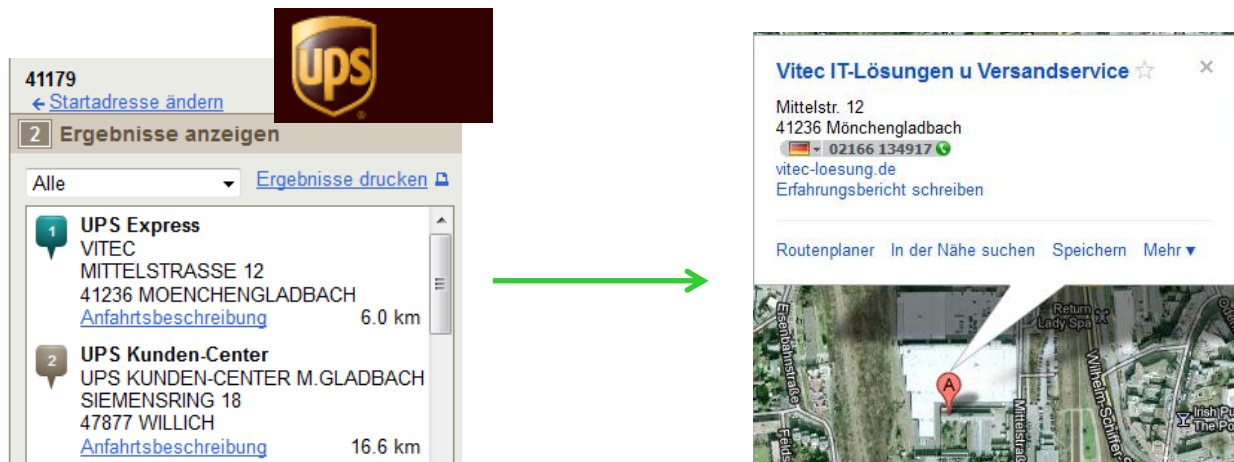


Bernd Peters
Konrad-Zuse-Ring 73
Mönchengladbach

Aber wer hat nun die Ersatzteile?

Die Prüfung der Versandadresse zeigt, dass alle angeforderten Teile an die gleiche Adresse verschickt wurden. Schauen wir uns diese Adresse mal in Google Maps an:

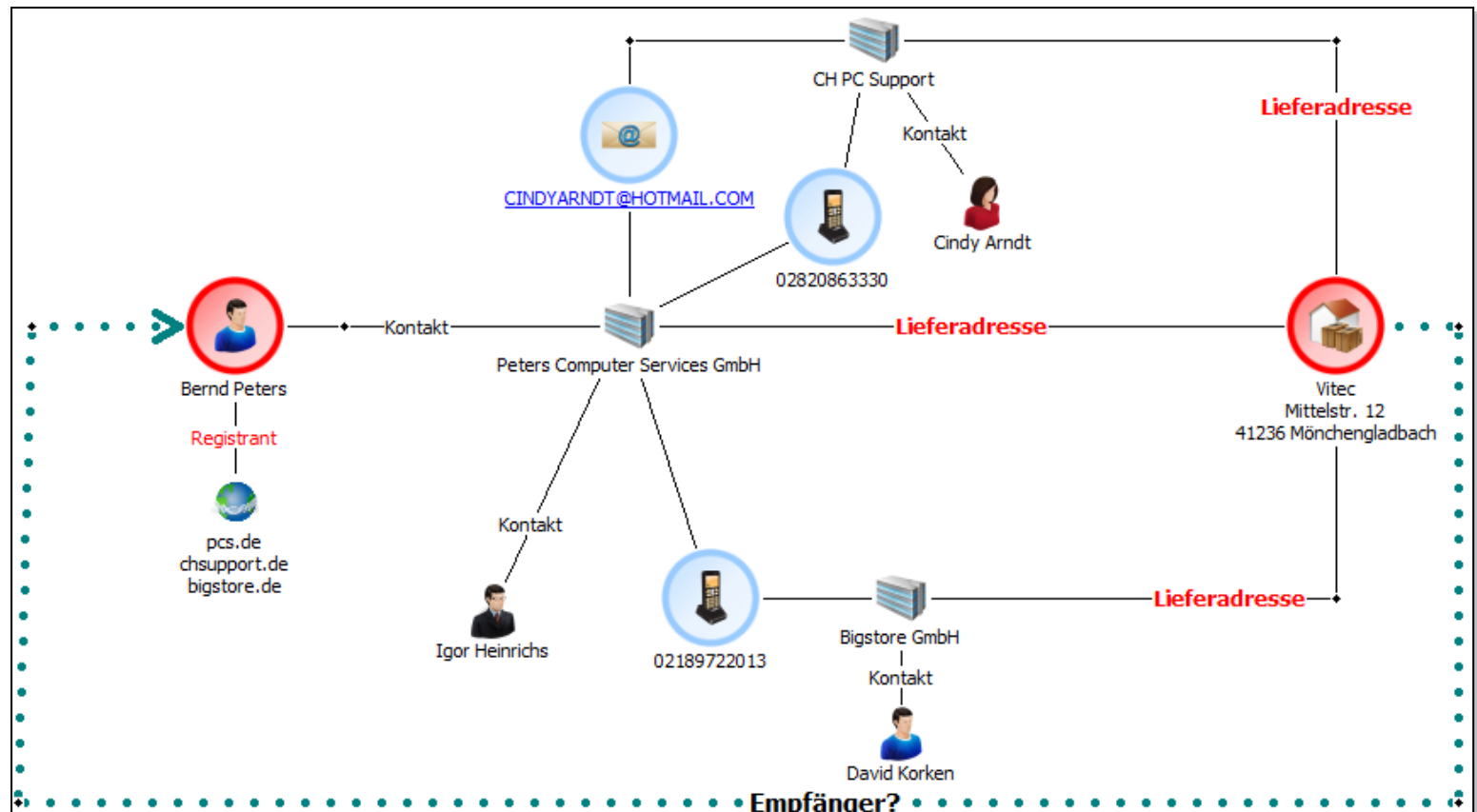
Alle Lieferungen gingen an ein Versandcenter von UPS:



The image shows a comparison between a UPS tracking interface and a Google Maps location. On the left, the UPS tracking page for package 41179 shows two results: 'UPS Express VITEC' at 'MITTELSTRASSE 12, 41236 MOENCHENGLADBACH' (6.0 km) and 'UPS Kunden-Center' at 'UPS KUNDEN-CENTER M. GLADBACH, SIEMENSRING 18, 47877 WILLICH' (16.6 km). A green arrow points from the first result to a Google Maps location pin 'A' on the right. The Google Maps pin is located at 'Mittelstr. 12, 41236 Mönchengladbach', with contact information '02166 134917' and 'vitec-loesung.de'.

| Ergebnis | Adresse | Abstand |
|---------------------|--|---------|
| 1 UPS Express VITEC | MITTELSTRASSE 12 41236 MOENCHENGLADBACH | 6.0 km |
| 2 UPS Kunden-Center | UPS KUNDEN-CENTER M. GLADBACH SIEMENSRING 18 47877 WILLICH | 16.6 km |

Ergebnis Linkanalyse



Fallabschluss



In Absprache mit dem Kunden und der örtlichen Polizei wurde auf Grundlage des Analyseberichts eine Durchsuchung an der primären Adresse von Bernd Peters durchgeführt.

Gefunden wurde dort eine hohe Anzahl entfernter Label, die zu den an den Hersteller gesandten Teilen passen. Zusätzlich unterhielt Herr Peters ein eigenes Lager mit günstig erworbenen, veralteten Ersatzteilen, die dem gleichen Muster entsprachen.



fragen?



Kontakt

corma GmbH

Jörn Weber

Nordpark

Heinz-Nixdorf-Str. 22

41779 Mönchengladbach

www.corma.de

mail@corma.de

Telefon: +49 (2161) 277 85-0

Fax: +49 (2161) 277 85-99

