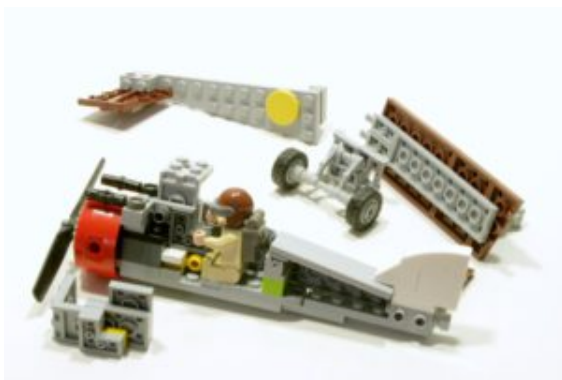


# Betriebsunterbrechungen durch Cyber-Attacken - eine der großen Gefahren für Unternehmen

Kelkheim, 20. Oktober 2017



Flickr: Mike

Seit nunmehr 6 Jahren identifizieren Risikoexperten aus verschiedenen Ländern für das Allianz Risk Barometer die wichtigsten Geschäftsrisiken für Unternehmen. Für den Report 2017 wurden mehr als 1.200 Risikomanager und Versicherungsexperten aus über 50 Ländern befragt.

Im fünften Jahr in Folge werden Betriebsunterbrechungen als das größte Risiko für Unternehmen angesehen. Betriebsunterbrechen führen zu Einkommensverlusten, die teilweise so hoch werden, dass die Betriebskosten nicht mehr gedeckt werden können, das Unternehmen Insolvenz anmelden muss. Wie hoch der Schaden letztlich sein kann, lässt sich für Unternehmen häufig schwer abschätzen.

Der durchschnittliche Verlust, den ein Unternehmen bei einer Betriebsunterbrechung erleidet, wird von den Versicherern mit 2,2 Millionen Euro angegeben - damit liegt der Schaden im Schnitt um mehr als ein Drittel höher als der Sachschaden auf den die Betriebsunterbrechung zurückgeht.

Die Gründe für eine Betriebsunterbrechung sind vielfältig. Zwar sind die

Hauptauslöser für Betriebsunterbrechungen immer noch Brände und Naturkatastrophen - und diese werden auch von den Unternehmen immer noch am meisten gefürchtet -, hinzukommen aber zunehmend Gefahren, bei denen die Unternehmen zwar keinen Sachschaden erleiden, die Verluste jedoch trotzdem gewaltig sind: Cybervorfälle und Terrorakte. Diese so genannten Nicht-Sachschäden-Risiken nehmen seit Jahren zu.

## **Cyber-Versicherung auch gegen Nicht-Sachschaden-Betriebsunterbrechungen**

Neben Bränden und Naturkatastrophen sind Cyber-Attacken die Hauptursache für eine Betriebsunterbrechung. Mit steigender Tendenz. Dass die Gefahr durch Betriebsunterbrechungen aufgrund von Cyberattacken zunimmt, korreliert mit der aktuellen Bewertung im Allianz Risk Barometer von Cyberangriffen als drittgrößte Gefahr für Unternehmen. Vor vier Jahren lag die Bedrohung durch Viren und Hacker-Angriffe nur auf Platz 15. Mittlerweile sind sich Risikomanager und Versicherer einig: Cyberrisiken sind ein fester Risikofaktor für Unternehmen und beinhalten längst nicht nur Datenverluste oder Verletzungen der Privatsphäre. Ein einziger Vorfall - ganz gleich, ob durch einen Fehler in der Betriebssoftware, menschliches Versagen oder ein mutwilliger Cyber-Angriff - kann schwerwiegende Folgen haben: Reputationsverlust, Verlust von Marktanteilen, Betriebsausfälle und und und. Zusätzlich können hohe Strafen auf Unternehmen zukommen, wenn durch eine Cyber-Attacke Datenschutzregeln verletzt wurden.

Zudem müssen die Unternehmen in unserer vernetzten Industrie nicht einmal selbst von einem Schaden oder einer Cyber-Attacke betroffen sein, damit es zu einer Betriebsunterbrechung kommt. Es genügt, wenn ein Zulieferer betroffen ist und daher die Lieferkette unterbrochen wird. Die Versicherer gehen davon aus, dass in den kommenden Jahren ein wesentlicher Anstieg von Betriebsunterbrechungen ohne eigentlichen Sachschaden zu sehen sein wird. Unternehmen müssen die sich daraus ergebenden Bedrohungen für ihre Existenz verstehen und darüber nachdenken, wie sie sich gegen diese Risiken absichern können. Eine Cyber-Versicherung ist wesentlicher Bestandteil dieser Abwehrstrategie.

## Über die gb.online gmbh

Die [gb.online gmbh](#) hat sich auf die berufliche Absicherung von Freelancern spezialisiert und bietet mit [www.easy-insure.eu](http://www.easy-insure.eu) das umfangreichste Online-Versicherungsportal für freie und beratende Berufe in Deutschland. Seit 2011 können Selbstständige und Unternehmen bis 1 Million Euro Umsatz pro Jahr hier ihre beruflichen Risiken versichern.

Steigt der Umsatz, und wird eine individuelle Lösung benötigt, so steht mit dem Schwesterunternehmen [groot bramel versicherungsmakler gmbh](#) ein verlässlicher Partner zur Seite, der seit über 25 Jahren Gewerbetreibende und industriellen Unternehmen in Versicherungsfragen vertritt. Die groot bramel versicherungsmakler gmbh ist in 18 Ländern vertreten und begleitet sie, wohin auch immer sich ihr Geschäftsfeld entwickelt.

## Kontaktdaten

gb.online gmbh  
Frankfurter Straße 93  
65779 Kelkheim

Ansprechpartner: [Lutz-Hendrik Groot Bramel](#), Geschäftsführer

Folgen Sie uns auch auf	
-------------------------	---

---

# [Surfen auf Reisen - wie sicher ist das öffentliche WLAN](#)

Durch das im Sommer 2016 geänderte Telemediengesetz soll die Anzahl offener Hotspots in Deutschland steigen. So praktisch das auch ist: offene Hotspots in Bahn- oder Flughäfen, in Cafés und Hotels bergen Risiken.



## **Risiken beim Surfen ber ffentliches WLAN**

Informatixonen ffentlicher Hotspots senden berwiegend unverschlselt. So knnen Hacker zum Beispiel sensible Daten wie zum Beispiel Passwrter ergreifen oder Schadsoftware auf das Gert einschleusen. Daher ist es ratsam, beim Surfen in fremden Netzen besonders vorsichtig zu sein. Nutzer sollten das automatische Einwhlen des Gerts in verfgbaren Hotspots deaktivieren und sich nur dann ins Netz einwhlen, wenn Sie es bentigen.

Wer auf Nummer sicher gehen mchte, kann sich vorher ber das Sicherheitsniveau des Hotspots informieren. Eine verschlseltete bertragung erhalten Nutzer zum Beispiel ber eine SSL-gesicherte Verbindung wie „HTTPS“ – erkennbar an einem grnen Schloss in der Adresszeile – oder ber ein Virtuell Private Netzwerk (VPN).

Ein VPN ermglicht eine verschlseltete Verbindung in ein sicheres Netzwerk. Das wiederum macht eine anonyme Kommunikation mglich.

## **Bankgeschfte sind tabu**

Das Abrufen vertraulicher Daten oder gar das erledigen von Bankgeschften in

öffentlichen Netzen sollte keinesfalls durchgeführt werden.

Wenn es unvermeidbar ist, dann unbedingt über eine VPN-Verbindung oder das Mobilfunknetz nutzen. Das ist zwar langsamer und kostet unter Umständen zusätzliches Geld, ist aber gegenüber dem öffentlichen WLAN der sicherere Weg. Darüber hinaus sollten der Virenschutz und die Firewall immer auf dem aktuellen Stand sein. Nicht zuletzt empfiehlt es sich, die Datei und Verzeichnisfreigabe im Gerät zu überprüfen und gegebenenfalls zu deaktivieren.

Schließlich ist es – je nach Konfiguration des Hotspots – möglich, dass das Gerät für andere sichtbar ist.

## **Über die [gb.online gmbh](#)**

Die [gb.online gmbh](#) hat sich auf die berufliche Absicherung von Freelancern spezialisiert und bietet mit [www.easy-insure.eu](http://www.easy-insure.eu) das umfangreichste Online-Versicherungsportal für freie und beratende Berufe in Deutschland. Seit 2011 können Selbstständige und Unternehmen bis 1 Million Euro Umsatz pro Jahr hier ihre beruflichen Risiken versichern.

Steigt der Umsatz, und wird eine individuelle Lösung benötigt, so steht mit dem Schwesterunternehmen [groot bramel versicherungsmakler gmbh](#) ein verlässlicher Partner zur Seite, der seit über 25 Jahren Gewerbetreibende und industrielle Unternehmen in Versicherungsfragen vertritt. Die groot bramel versicherungsmakler gmbh ist in 18 Ländern vertreten und begleitet sie, wohin auch immer sich ihr Geschäftsfeld entwickelt.

## **Kontaktdaten**

gb.online gmbh

Frankfurter Straße 93

65779 Kelkheim

Ansprechpartner: [Lutz-Hendrik Groot Bramel](#), Geschäftsführer

# Wie Sie zum Best-Practice-Unternehmen in Sachen Cyber-Sicherheit werden

Kelkheim, 14. März 2017



Flickr: elhombredenegro

Nach dem „Hiscox Cyber Readiness Report 2017“ sind nur 20 Prozent der deutschen Unternehmen gut auf eine Cyber-Attacke vorbereitet. Sie werden als so genannte „Cyber-Experten“ bewertet. Doch was unterscheidet diese 20 Prozent von den 62 Prozent der Unternehmen, die so ungenügend auf Cyber-Attacken vorbereitet sind, dass sie als „Cyber-Anfänger“ kategorisiert werden bzw. den 18 Prozent, die immerhin schon „Cyber-Fortgeschrittene“ sind?

## **Es gibt noch viel zu tun**

Den deutschen Unternehmen ist mehrheitlich bewusst, dass sie noch viel zu tun haben, wenn es um den Bereich IT-Sicherheit geht. Deshalb plant die Mehrheit

von ihnen für die kommenden 12 Monate auch mindestens 5 Prozent mehr Budget für Investitionen in die Sicherheit ihrer IT ein, dabei liegt der Fokus auf neuen Sicherheitstechnologien. 61 Prozent wollen gezielt ihre Schwachstellen angehen. Aber was kann man ihnen empfehlen? Ein Blick auf die 20 Prozent Best-Practice-Unternehmen zeigt, was diese besser machen.

Die meisten der befragten Unternehmen sind, wenn es um die Sicherheitstechnologien geht bereits gut aufgestellt. Hier gibt es den geringsten Nachholbedarf; nur im Bereich Nachrichtenverschlüsselung könnte es noch besser werden.

### **Was machen Cyber-Security-Experten besser?**

Der größte Unterschied zwischen Cyber-Anfängern und -Experten liegt in den Bereichen Strategie und Prozesse. Während in den Best-Practice- Unternehmen rund 88 Prozent der Befragten Cyber-Sicherheit als Chefsache ansehen, sind es bei den als Anfänger eingestuften Unternehmen nur 58 Prozent.

Bei den Experten wird also das Top-Management in die Cyber-Strategie miteinbezogen und ist wesentlich an der Entwicklung eines formalisierten Cyber-Sicherheitsstrategie beteiligt. Es sind klar definierte Strukturen und Prozesse entwickelt worden, die allen bekannt sind.

Zudem gibt es Cyber-Security-Guidelines für Mitarbeiter, Partner und Externe. Alle werden regelmäßig geschult und getestet, um zu gewährleisten, dass die Richtlinien eingehalten werden. Die Schulung der Mitarbeiter ist dabei insgesamt ein wesentlicher Teil des Cyber-Sicherheitskonzepts. Denn nur sensibilisierte und gut trainierte Mitarbeiter können mithelfen, Attacken zu vermeiden. Die Personalabteilung ist mit eingebunden und sorgt für die Weiterbildung der Mitarbeiter.

Der letzte Baustein eines umfassenden Cyber-Risk-Managements ist eine Cyber-Versicherung. Fast zwei Drittel der „Cyber-Experten“ verfügen über eine Cyber-Police. Ein Großteil der Experten plant zudem, den Cyber-Schutz in den nächsten 12 Monaten weiter auszubauen. Denn den Experten ist bewusst: Ganz gleich, wie viel sie in IT-Sicherheitstechnologien und in die Schulung der Mitarbeiter investieren, die Gefahr eines Cyber-Angriffes kann man zwar reduzieren, aber nie ganz eliminieren. Daher schützen sie sich durch eine Cyber-Versicherung vor den Restrisiken.

## Über die gb.online gmbh

Die [gb.online gmbh](#) hat sich auf die berufliche Absicherung von Freelancern spezialisiert und bietet mit [www.easy-insure.eu](http://www.easy-insure.eu) das umfangreichste Online-Versicherungsportal für freie und beratende Berufe in Deutschland. Seit 2011 können Selbstständige und Unternehmen bis 1 Million Euro Umsatz pro Jahr hier ihre beruflichen Risiken versichern.

Steigt der Umsatz, und wird eine individuelle Lösung benötigt, so steht mit dem Schwesterunternehmen [groot bramel versicherungsmakler gmbh](#) ein verlässlicher Partner zur Seite, der seit über 25 Jahren Gewerbetreibende und industriellen Unternehmen in Versicherungsfragen vertritt. Die groot bramel versicherungsmakler gmbh ist in 18 Ländern vertreten und begleitet sie, wohin auch immer sich ihr Geschäftsfeld entwickelt.

## Kontaktdaten

gb.online gmbh  
Frankfurter Straße 93  
65779 Kelkheim

Ansprechpartner: [Lutz-Hendrik Groot Bramel](#), Geschäftsführer

Folgen Sie uns auch auf	
-------------------------	--



# Hiscox Cyber Readiness Report 2017 - Mehrheit deutscher Unternehmen als „Cyber-Anfänger“ einzustufen

Kelkheim, 03. März 2017

**Der „Hiscox Cyber Readiness Report 2017“ ist erschienen - und bringt teilweise erschreckende Erkenntnisse zu Tage. Fast 40 Prozent der deutschen Unternehmen hinken im internationalen Vergleich deutlich hinterher, wenn es um Cyber-Sicherheit geht.**



Flickr: elhombredenegro

Für den „Hiscox Cyber Readiness Report 2017“ wurden über 3000 Führungskräfte, Abteilungsleiter, IT-Manager und andere für die Cyber-Sicherheit verantwortliche Mitarbeiter von Unternehmen befragt; je rund 1000 in

Deutschland, Großbritannien und USA. Die Befragten sollten eine Selbsteinschätzung zu ihrer Cyber-Security-Strategie, ihren Ressourcen, ihren Prozessen und ihrer Technologie abgeben. Auf Basis dieser Einschätzung wurden die Unternehmen in die Kategorien „Cyber-Anfänger“, „Cyber-Fortgeschrittene“ und „Cyber-Experten“ eingeteilt. Als Anfänger zählt, wer nur unzureichend auf Cyber-Attacken vorbereitet ist, Cyber-Fortgeschrittene sind zumindest teilweise für einen Angriff gewappnet. Nur wer gut geschützt auf einen Cyber-Angriff reagieren kann, gilt als Cyber-Experte.

## **Deutschland ist Nachzügler bei IT-Sicherheit**

Das Bild, das sich abzeichnete, ist eindeutig: Deutschland ist Nachzügler, was das Thema IT-Sicherheit angeht. Während in den USA 40 Prozent der Unternehmen als „Cyber-Anfänger“, also als unzureichend gegen Cyber-Attacken geschützt, einzustufen sind, sind es in Deutschland ganze 62 Prozent. Großbritannien liegt mit 57 Prozent in der Mitte.

Als gut geschützt können in Deutschland lediglich 20 Prozent der Unternehmen angesehen werden. Im Vergleich: 44 Prozent, also mehr als doppelt so viele, der befragten US-Unternehmen sind gut gegen Cyber-Attacken gerüstet, in Großbritannien sind es 26 Prozent.

## **Mehr als die Hälfte der deutschen Unternehmen wurde schon einmal attackiert**

Dieses schlechte Abschneiden der deutschen Unternehmen ist umso erstaunlicher, wenn man sich dazu die Zahlen der Cyber-Attacken im vergangenen Jahr anschaut: 56 Prozent der befragten deutschen Unternehmen haben 2016 einen Angriff auf ihre Netzwerke und Daten verzeichnet.

Besonders oft werden hierzulande Unternehmen aus der Fertigungsindustrie, den Medien sowie den Branchen Kommunikation und Technologie Ziel von Cyber-Attacken. Hier haben jeweils 65 Prozent der befragten Unternehmen mindestens einen Cyber-Angriff entdeckt; knapp dahinter liegt die Finanzdienstleistungsbranche mit 64 Prozent.

## **Unterschätztes Risiko Mitarbeiter**

Den Cyber-Angriff, den Unternehmen befürchten, ist die typische Hacker-Attacke

von außen. Tatsächlich verursachen externe Angriffe mit 38 Prozent auch die meisten Cyber-Zwischenfälle. Auf Platz 2 und 3 folgen aber schon Zwischenfälle, die durch die eigenen Mitarbeiter hervorgerufen wurden: absichtlich oder unabsichtlich. Rund 20 Prozent der von Cyber-Attacken betroffenen Unternehmen stellten fest, dass der Verantwortliche innerhalb der eigenen Organisation auszumachen war; weitere 14 Prozent berichteten von verlorenen oder gestohlenen mobilen Devices, wie Firmenhandys oder -tablets, als Ursache.

Obwohl ein Fünftel der Cyber-Attacken intern verschuldet werden, vernachlässigen deutsche Unternehmen das Thema Mitarbeiterschulung bzw. -sensibilisierung. Nur ein Viertel der Unternehmen führen verpflichtende Cyber-Trainings durch. Allerdings hat der Report hier auch etwas Positives zu berichten: Mehr als die Hälfte (57 Prozent) der befragten deutschen Unternehmen planen in den kommenden 12 Monaten mehr in die Cyber-Security-Schulung der Mitarbeiter zu investieren.

### **Cyber-Experten verfügen über eine Cyber-Versicherung**

Dass Deutschland beim Thema Cyber-Security noch einiges aufzuholen hat, zeigt auch ein Blick auf die Anzahl der abgeschlossenen Cyber-Versicherungen. Während in den USA 55 Prozent der Unternehmen eine Cyber-Police besitzen, sind es in Deutschland nur 30 Prozent. Immerhin wollen etwa ein Drittel der deutschen Unternehmen, die noch über keine Cyber-Versicherung verfügen, dies in den kommenden 12 Monaten nachholen. Doch rund 40 Prozent glauben, sie bräuchten keine Versicherung: entweder weil sie überzeugt sind, gut genug abgesichert zu sein, nicht darauf vertrauen, dass der Versicherer im Schadenfall auch zahlen würde oder nicht wissen, dass es ein spezielles Versicherungsprodukt gibt, das Cyber-Risiken abdeckt.

### **Was kann Deutschland tun, um international den Anschluss zu bekommen?**

Wie der Report zeigt, gibt es auch einige deutsche Unternehmen, die zu den Cyber-Experten gehören. Was können die Unternehmen aus den Kategorien Anfänger und Fortgeschrittene von den Experten lernen? Was die Experten besser machen erfahren Sie in unseren nächsten Artikel.

## Über die gb.online gmbh

Die [gb.online gmbh](#) hat sich auf die berufliche Absicherung von Freelancern spezialisiert und bietet mit [www.easy-insure.eu](http://www.easy-insure.eu) das umfangreichste Online-Versicherungsportal für freie und beratende Berufe in Deutschland. Seit 2011 können Selbstständige und Unternehmen bis 1 Million Euro Umsatz pro Jahr hier ihre beruflichen Risiken versichern.

Steigt der Umsatz, und wird eine individuelle Lösung benötigt, so steht mit dem Schwesterunternehmen [groot bramel versicherungsmakler gmbh](#) ein verlässlicher Partner zur Seite, der seit über 25 Jahren Gewerbetreibende und industriellen Unternehmen in Versicherungsfragen vertritt. Die groot bramel versicherungsmakler gmbh ist in 18 Ländern vertreten und begleitet sie, wohin auch immer sich ihr Geschäftsfeld entwickelt.

## Kontaktdaten

gb.online gmbh  
Frankfurter Straße 93  
65779 Kelkheim

Ansprechpartner: [Lutz-Hendrik Groot Bramel](#), Geschäftsführer

Folgen Sie uns auch auf	
-------------------------	--

---

**Endlich Klarheit: IT-Freelancer nicht vom neuen**

# Arbeitnehmerüberlassungsgesetz betroffen

Kelkheim, 7. Dezember 2016



Flickr: Dennis Ngan

Es ist soweit: Das neue Arbeitnehmerüberlassungsgesetz wurde am 21. Oktober beraten und soll zum 1. April 2017 in Kraft treten. Die geänderte Fassung soll Leiharbeiter dafür schützen, dauerhaft zu niedrigeren Löhnen als die Stammebelegschaft zu arbeiten oder durch Werkverträge in eine abhängige Scheinselbstständigkeit gedrängt zu werden. Mit der beschlossenen Fassung gibt es nun endlich Rechtssicherheit für zig Tausende von IT-Freelancern, die über Werkverträge ihre Projekte abwickeln. Denn sie sind davon ausgenommen.

Werkverträge gerieten ins Blickfeld der Politik, da diese in den vergangenen Jahren verstärkt dazu genutzt wurden, um Leiharbeitsverträge und Sozialversicherungsbeiträge zu umgehen. Statt in einem regulären Arbeitsverhältnis angestellt, erhielten Leiharbeiter einen Werkvertrag und wurden als (Schein-)Selbstständige beauftragt. So konnten Arbeitgeber das Risiko

gänzlich auf den Leiharbeiter verlagern. Mit dem neuen Arbeitnehmerüberlassungsgesetz soll daher nicht nur die Leiharbeit besser geregelt, sondern auch der Missbrauch von Werksverträgen eingeschränkt werden.

### **Lange Zeit herrschte Unsicherheit bei IT-Freelancern und Unternehmen**

Lange war unklar, ab wann bei der Arbeit mit Werkverträgen ein Beschäftigungsverhältnis zu Stande käme. Genau dies hat bei vielen Freiberuflern Unsicherheit ausgelöst. Denn gerade im Bereich IT arbeiten Freelancer häufig auf Projektbasis lange Zeit nur für einen Auftraggeber und verrichten ihre Arbeit zudem bei diesem im Unternehmen. Damit könnte die Gefahr bestehen, als scheinselfständig eingestuft zu werden oder der geschlossene Werks- oder Dienstvertrag als ein Versuch gewertet werden, eine Anstellung zu umgehen. Damit würde sich der selbstständige IT-Freelancer auf einmal gegen seinen Willen in einem Angestelltenverhältnis wiederzufinden.

Dies war auch für den Auftraggeber ein großer Unsicherheitsfaktor. Schließlich hätte dies hohe Sozialversicherungsnachzahlungen bedeuten können.

Am 21. Oktober hat nun der Bundestag über eine überarbeitete Version des neuen Arbeitnehmerüberlassungsgesetzes beraten und entschieden: Leiharbeit wird gesetzlich auf 18 Monate begrenzt; wenn die betroffenen Arbeitnehmer tarifvertraglich behandelt werden, kann diese Grenze auf 24 Monate erhöht werden. Nach 9 Monaten Einsatz werden Leiharbeiter dabei den regulär angestellten Mitarbeitern gleichgestellt (Equal-Pay). Werkverträge werden immer im Einzelfall begutachtet.

### **Nun ist klar: IT-Freelancer sind nicht vom Arbeitnehmerüberlassungsgesetz betroffen**

Das Wichtige für IT-Freelancer und andere Freiberufler ist: Es wurde eindeutig festgehalten, das neue Gesetz ziele nicht darauf ab, die unternehmerische Tätigkeit von Wissensarbeitern und Beratungsunternehmen einzuschränken. „Die Neuregelung solle dem sachgerechten Einsatz von Werk- und Dienstverträgen in den zeitgemäßen Formen des kreativen oder komplexen Projektgeschäfts nicht entgegenstehen, wie sie zum Beispiel in der Unternehmensberatungs- oder IT-

Branche in Optimierungs-, Entwicklungs- und IT-Einführungsprojekten anzutreffen seien“ ([Bundestagsdrucksache Nr. 18/10064, S. 13](#)).

Höherqualifizierte Selbstständige, die freiwillig und gerne selbstständig sind, werden also nicht von dem neuen Arbeitsüberlassungsgesetz betroffen sein. Das bedeutet: IT-Freelancer, wie auch Ingenieure, Unternehmensberater und andere Wissensarbeiter, können aufatmen: Projektarbeit, wie sie in der digitalen Arbeitswelt Gang und Gäbe ist, wird weiterhin möglich sein und die Arbeit an einem großen, monatelangen IT-Projekt gefährdet nicht die Selbstständigkeit der Freiberufler.

## Über die [gb.online gmbh](#)


Die [gb.online gmbh](#) hat sich auf die berufliche Absicherung von Freelancern spezialisiert und bietet mit [www.easy-insure.eu](#) das umfangreichste Online-Versicherungsportal für freie und beratende Berufe in Deutschland. Seit 2011 können Selbstständige und Unternehmen bis 1 Million Euro Umsatz pro Jahr hier ihre beruflichen Risiken versichern.

Steigt der Umsatz, und wird eine individuelle Lösung benötigt, so steht mit dem Schwesterunternehmen [groot bramel versicherungsmakler gmbh](#) ein verlässlicher Partner zur Seite, der seit über 25 Jahren Gewerbetreibende und industriellen Unternehmen in Versicherungsfragen vertritt. Die groot bramel versicherungsmakler gmbh ist in 18 Ländern vertreten und begleitet sie, wohin auch immer sich ihr Geschäftsfeld entwickelt.

## Kontaktdaten

gb.online gmbh  
Frankfurter Straße 93  
65779 Kelkheim

Ansprechpartner: [Lutz-Hendrik Groot Bramel](#), Geschäftsführer

Folgen Sie uns auch auf	
-------------------------	--