

# Wirksamer Schutz gegen Cyberkriminalität

**Hackerattacken, Datendiebstahl oder Computermisbrauch gehören in unserem digitalen Zeitalter zu gängigen Berufsrisiken in Unternehmen. Hohe Schadenersatzforderungen, Bußgelder oder Vertragsstrafen können die Folge sein, die sich jedoch mit einigen Präventionsmaßnahmen vermeiden lassen können.**

Für die Führungskräfte ist es wichtig, mögliche Cyberrisiken im Unternehmen richtig einzuschätzen, denn falls es zu Cyberattacken wie Datendiebstahl oder Computerbetrug kommen sollte, droht nicht nur der Schaden für das Unternehmen, sondern auch für die Geschäftsleitung und für leitende Angestellte, die sie einem solchen Fall ein „Organisationsverschulden“ trifft und persönlich haftbar gemacht werden können.



## **So bauen Sie ein digitales Schutzschild für Ihr Unternehmen**

Das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ bietet eine erste Hilfestellung, wenn es um IT-Sicherheit in Unternehmen geht. Es informiert über zahlreiche Meldepflichten bei Behörden, die eingehalten werden

sollten, um Bußgelder zu vermeiden. Ebenso gibt es umfangreiche Ratschläge, welche Schritte bei einem Schadensfall nötig sind.

Für die Geschäftsführung ist es häufig schwierig, alle Risiken von Cyberkriminalität genau einzuschätzen. Gleichzeitig sind umfangreiche IT-Sicherheitsvorkehrungen notwendig, um ein Unternehmen gegen Hackerangriffe zu schützen. Aus diesem Grund empfiehlt es sich, Fachkräfte für IT-Sicherheit einzustellen. Diese können Sicherheitslücken schnell erkennen, Firewalls überprüfen, die IT-Infrastruktur sorgfältig warten und ebenso das Sicherheitsbewusstsein von Mitarbeitern verstärken sowie Datenschutzrichtlinien wahren.

Kommt es trotz aller Präventionsmaßnahmen zu einer Cyberattacke und es werden beispielsweise sensible Kundendaten gestohlen, drohen dem Unternehmen sowie der Geschäftsführung und leitenden Angestellten Bußgelder, Vertragsstrafen oder hohe Schadensersatzforderungen. Hier kann eine Vermögensschadenshaftpflichtversicherung, die Directors & Officer Police finanzielle Forderungen abdecken.

Sollte ein Cyberbetrug existenzbedrohend für ein Unternehmen sein, ist es sinnvoll zu prüfen, ob eine Cyber-Deckung finanziellen Schutz bietet.

Eine gängige IT-Haftpflichtversicherung empfiehlt sich in jedem Fall, da sie für Schäden bei Kunden und Geschäftspartnern aufkommen kann.

Sind alle Risiken sorgfältig durchdacht und mit entsprechenden Versicherungen abgedeckt sowie professionelle IT-Sicherheitsmitarbeiter eingestellt, die sich um alle sicherheitsrelevanten Vorgänge kümmern, ist ein Unternehmen optimal gegen Cyberattacken gerüstet.

## 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	 
----------------------------	--