



# Projekt HOLISTIK

IT-Security, ganzheitliche Betrachtung modular, sicher und wirkungsvoll

## Sicherheit von außen und innen

Ein System ist sicher,  
solange niemand von ihm weiß.

1. Analyse & Beratung
2. Sicherheit erhöhen
3. Begleiten bei Notfällen
4. Normalbetrieb wiederherstellen
5. Rechtlichen Rahmen schaffen
6. Versicherungsleistungen

## Prävention

Wieviel Sicherheit darf es sein?

Gab es in Ihrem Unternehmen bereits einen Sicherheitsvorfall? Viele Unternehmen wähen sich sprichwörtlich „in Sicherheit“ und verneinen diese Frage spontan. Dabei wird nicht berücksichtigt, dass IT-Angriffe oft monate- bis jahrelang unentdeckt bleiben (Quelle: Bundesamt für Sicherheit in der Informationstechnik, Lagebericht 2014) und Cyber-Kriminelle sich nicht auf große und bekannte Unternehmen beschränken. Im Gegenteil sind mittelständische Firmen oft leichter zu „knacken“ und z.B. im Erpressungsfall eher bereit, für die Rückgabe ihrer Daten zu zahlen.



### Ist Ihr Unternehmen gefährdet?

Wenn Sie eine oder mehrere der folgenden Fragen mit „ja“ beantworten, sollten Sie Ihre Sicherheit überprüfen lassen.

- ⇒ Speichern Sie geschäftliche und persönliche Daten (auch Ihrer Mitarbeiter, Kunden, Lieferanten und anderer Partner) auf einem Computer?
- ⇒ Versenden und empfangen Sie geschäftliche Emails?
- ⇒ Hat Ihr Unternehmen eine Homepage?
- ⇒ Sind Sie oder Ihre Mitarbeiter (privat) in sozialen Netzwerken aktiv und geben an, wo oder in welcher Funktion sie arbeiten?
- ⇒ Beeinträchtigt ein mehrtägiger IT-Ausfall Ihre Arbeit und wird vielleicht sogar existenzbedrohend?
- ⇒ Denken Sie über eine „Cyber-Versicherung“ zur Reduzierung des Restrisikos und zur Absicherung von IT-Schäden und Datenschutzverletzungen nach?

### Sicherheitsprüfung, wie läuft das ab?

#### Modul 01

#### Analyse & Beratung

- ⇒ Analyse der individuellen Risiken
- ⇒ Beratung zur Risikominimierung und Schwachstellenbehebung
- ⇒ Erstellen eines angemessenen Sicherheitskonzeptes

#### Modul 02

#### Sicherheit erhöhen

- ⇒ Umsetzung der Maßnahmenempfehlungen
- ⇒ Penetrationstests
- ⇒ Sensibilisieren von Mitarbeitern
- ⇒ Vorbereitung und Durchführung einer Zertifizierung
- ⇒ Notfallmanagement und Notfallplanung
- ⇒ Finanzielle und rechtliche Absicherung des Restrisikos



### Lassen Sie es nicht soweit kommen.

Wenn der Notfall eintritt, sollte man gegen jeglichen Instinkt zunächst Ruhe bewahren. Diese Besonnenheit und Routine im Ernstfall erreichen Sie, wenn Sie mögliche Vorfälle bereits durchgespielt und die notwendigen Schritte und Gegenmaßnahmen im Vorfeld in einem Notfallhandbuch dokumentiert haben.

Wir helfen Ihnen bei der Erstellung dieser Dokumentationen und begleiten Sie im Ernstfall, wir stehen Ihnen in allen Krisensituationen beratend und unterstützend beiseite.



### Im Ernstfall, was steht an?

#### Begleiten bei Notfällen

#### Modul 03

- ⇒ Unterstützung bei der Gewährleistung von Handlungs- und Rechtssicherheit
- ⇒ Koordinierung von Abteilungen, Behörden und Medienvertreter
- ⇒ Mitarbeit bei der Etablierung eines Krisenstabs, bzw. im Krisenstab

#### Normalbetrieb wiederherstellen

#### Modul 04

- ⇒ Unterstützung beim Wiederanlauf
- ⇒ Feststellen des Schadensausmaßes und Schadensbehebung
- ⇒ Forensische Analyse und Beweissicherung

#### Rechtlichen Rahmen schaffen

#### Modul 05

- ⇒ Täter rechtlich belangen
- ⇒ Beratung in Rechtsfragen, Vermeidung / Reduzierung des Haftungsrisikos
- ⇒ Zusammenarbeit mit Behörden, Meldepflicht

#### Versicherungsleistungen

#### Modul 06

- ⇒ Übernahme der Kosten infolge eines Cyber-Angriffs
  - ⇒ Eigenschäden (z.B. Rechtsanwälte, Benachrichtigung Geschädigter)
  - ⇒ Erfüllung bzw. Abwehr eines Haftpflichtanspruches durch Datenrechtsverletzung
  - ⇒ Betriebsunterbrechung, Datenwiederherstellung
  - ⇒ Weitere Leistungen (je nach Versicherungspaket)



Dr. Thiele IT-Beratung  
Adresse: 64372 Ober-Ramstadt  
Rodauer Straße 5  
Tel/Fax: 06162 1052 / 1055  
Email: [cyber@dr-thiele.it](mailto:cyber@dr-thiele.it)  
Web: [www.dr-thiele.it](http://www.dr-thiele.it)

#### Zertifizierte Sicherheit: Analyse, Beratung, Sensibilisierung und Forensik

Die *Dr. Thiele IT-Beratung* deckt auf, welchen Gefährdungen Ihr Unternehmen ausgesetzt ist, wie Cyber-Kriminelle Schwachstellen ausnutzen, ob Ihr aktueller Schutz wirkt und wie Ihre Sicherheit mit Sofort-Maßnahmen angemessen und wirtschaftlich gesteigert werden kann. Als mehrfach zertifizierte Cyber-Security-Experten und Datenschützer unterstützen wir Sie von der Erstanalyse über die Erstellung eines Maßnahmenkatalogs bis hin zur Schadensbehebung und Ursachenermittlung (Forensik). Wir begleiten Sie im Ernstfall.

24/7 - im Notfall sind wir rund um die Uhr für Sie da.

Volle Unterstützung und schnelle Reaktion im Schadensfall.



Global Service Group GmbH  
Adresse: 64354 Reinheim  
Darmstädter Str. 53  
Tel/Fax: 06162 1051 / 1055  
Email: [info@gsg-edv.de](mailto:info@gsg-edv.de)  
Web: [www.gsg-edv.de](http://www.gsg-edv.de)

#### Kompetente Realisierung: Hard- und Softwarelösungen, Maßnahmenumsetzung

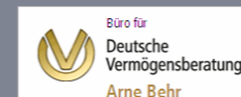
*GSG Global Service Group* ist das EDV-Systemhaus für alle Anforderungen rund um Ihre IT-Infrastruktur wie z.B. PCs, Laptops, Mobils, Telefon- und Kommunikationsanlagen, Server und Software, auch bei individuellen Bedürfnissen. Wir übernehmen Installation, Wartung und Reparatur sowie Monitoring und Sofort-Hilfe im Ernstfall, im Fokus stehen dabei stets Ihre IT-Sicherheit und das aktive Notfallmanagement. Besondere Erfahrung haben wir in der Betreuung mittelständischer Unternehmen.



RA Ralf Hillgärtner  
Adresse: Hagstraße 13  
35396 Gießen  
Telefon: 0641 3205696  
Fax: 0641 95054411  
Handy: 0151 64568553  
Email: [Kanzlei.Hillgaertner@gmail.com](mailto:Kanzlei.Hillgaertner@gmail.com)

#### Rechtssicher agieren: IT-Rechtsberatung und Unterstützung im Schadensfall

Aus den unterschiedlichsten gesetzlichen Bestimmungen sind die geeigneten Paragraphen zusammen zu suchen. Nur wer sich in diesem Dschungel zurechtfindet und entsprechend geeignete Sicherheitsvorkehrungen trifft, kann sich vor eventuellen rechtlichen Konsequenzen schützen. Die *Rechtsanwaltskanzlei Hillgärtner* zeigt Ihnen auf, wie sie diese Rechtssicherheit erlangen können, berät Sie in allen IT-Rechtsfragen und hilft Ihnen schon im Vorfeld, Ihr Haftungsrisiko so gering wie nur möglich zu halten. Sollte es dennoch einmal zu einem Schadensfall kommen, vertritt die Kanzlei Sie auch gerne anwaltlich für Ihr gutes Recht.



Mag.phil. Arne Behr,  
Vermögensberater  
Adresse: Rebenstraße 18  
64646 Heppenheim  
Telefon: 06252 603077  
Mobil: 0171 9531257  
Email: [arne.behr.4136220@dvag.de](mailto:arne.behr.4136220@dvag.de)

#### Restrisiko absichern: Cyber-Versicherung für den „Fall der Fälle“

Als Unternehmens- und Vermögensberater für klein- und mittelständische Unternehmen, berate ich meine Kunden unter anderem im Risikomanagement. Spezielle Cyber-Risk-Policen für Dienstleistungs-, Beratungs- und IT-Unternehmen sichern den finanziellen Ernstfall ab, wenn ein Cyber-Angriff trotz technischer Vorsorge erfolgreich war. Leistungsfähige Vermögensschadenkonzepte für beratende Berufe und Elektronikversicherungen für die mobile Elektronik runden den Schutz ab. Als Ergänzung sichert ein professionelles Rechnungsmanagement und Factoring die Liquidität meiner Kunden.