CYBER-ABSICHERUNG

WELCHE LEISTUNGSINHALTE SIND ENTHALTEN?

1.HAFTPFLICHT (Schäden Dritter)
Folgende Pflichtverletzungen sind absicherungsrelevant:

- ✓ Datenangriff
- ✓ Rechtsverletzung
- ✓ Ausspähung
- ✓ Verhinderter Zugang
- ✓ Rufschädigung

2. EIGENSCHÄDEN

Versichert sind außerdem Eigenschäden in Zusammenhang mit einem Hacker- Angriff, DoS-Attacken, Computermissbrauch, Diebstahl von Datenträgern sowie einer sonstigen Datenrechtsverletzung. Dazu gehören z.B.:

- ✓ Computer-Forensik–Spezialisten
- ✓ Benachrichtigungskosten Ihrer Kunden/Mandanten
- ✓ Kreditschutz- und Kreditüberwachungsservices
- ✓ Wiederherstellung von Daten und Netzwerken
- ✓ Reputationsschäden und Kosten für Krisenkommunikation
- ✓ Cyber Erpressung
- ✓ Cyber Vandalismus
- ✓ Betriebsunterbrechung und Folgeschäden

SUBVENTION VON PRÄVENTIVEN BERATUNGSMASSNAHMEN

Übernahme der Kosten für
IT-Experten, die Sicherheitslücken schließen oder den Sachverhalt aufklären und gerichtsverwertbar dokumentieren.

Übernahme der Kosten für einen Rechtsbeistand
oder die Vermittlung von Experten einer renommierten Wirtschaftskanzlei.

DEN PASSENDEN ANBIETER ERHALTEN SIE BEI UNS!

- Langjährige Erfahrung im Bereich Cyber Risk Management.
- Genaue Einschätzung des Risikopotenzials.
- Analyse Ihrer individuellen Bedürfnisse.
- Klare und transparente Vertragsgestaltung mit umfassender Absicherung.
- Speziell auf den deutschen Markt zugeschnittene Absicherungen.
- Individuelle Betreuung durch einen persönlichen Schadenregulierer.
- Hilfe durch ein Netzwerk externer Spezialisten.
- Exklusive Zusammenarbeit der Versicherer mit führenden IT-Sicherheits und Krisenberatungsunternehmen.
- Besonderes Know-how im Bereich klein- und mittelständischer Unternehmen.
- Sicherstellung der Funktionsfähigkeit Ihrer Homepage durch zeitnahe Reparatur bzw. Ersatz.

STERK
FINANCIAL PLANNING

Ein Thema! Viele Fragen.

Deshalb sind wir genau der richtige Ansprechpartner für Sie und stehen Ihnen mit unserer Expertise sehr gerne zur Seite.

Wir freuen uns auf das persönliche Gespräch mit Ihnen.
Ihr Ingo Sterk mit Team

STERK FINANCIAL PLANNING GMBH
Im Wiesengrund 27
D-78234 Engen

Telefon +49 (0) 77 33 - 98 199 - 60
Telefax +49 (0) 77 33 - 98 199 - 65

Email dialog@sterk-fp.de
Web www.sterk-fp.de

STERK
FINANCIAL PLANNING

CYBER RISK MANAGEMENT

EIN HACKERANGRIFF KANN IHR UNTERNEHMEN IN DIE STEINZEIT VERSETZEN

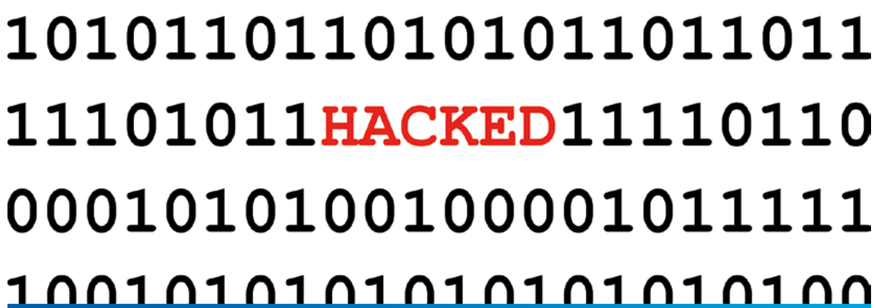
AUFBAU EINES CYBER RISK MANAGEMENTS

Digitale Risiken, wie Hackerangriffe oder Datenverluste, sind allgegenwärtig. Jeder kann, unabhängig der Größe seines Unternehmens, davon betroffen sein. Das Ausmaß der, durch einen Hackerangriff entstehenden, Probleme ist vielen nicht bewusst. Bei kleinen und mittelständischen Unternehmen kann es überlebenswichtig sein, ein funktionierendes Cyber Risk Management zur Absicherung zu haben. Ein vollzogener Angriff hinterlässt im Durchschnitt einen Schaden in Höhe von bis zu 41.000 Euro. Dies kann auch ein kleines Unternehmen schnell an den Rand der Existenz bringen.

FÜR WEN IST EINE CYBERABSICHERUNG INTERESSANT?

Für ALLE Unternehmen, Selbstständige und Freiberufler, die:

a) Personenbezogene / vertrauliche Daten speichern, bearbeiten oder verwalten
b) von Computernetzwerken, digitalen Informationen oder dem Internet abhängig sind
c) Online-Geschäfte tätigen
d) Informationen in elektronischer Form veröffentlichen



RISIKEN FÜR SIE UND IHR UNTERNEHMEN!

TROJANER UND WÜRMER
Sie sind der Klassiker unter den Cyber-Schädlingen. Während sie sich unbemerkt in Ihr System einnisten, klauen sie persönliche Daten und/oder infizieren Ihre E-Mails. Installierte Anti- Viren- Programme schützen zwar, trotzdem bleibt nahezu die Hälfte aller Schädlinge unbemerkt!

VIREN-BAUKÄSTEN (EXPLOSIT KITS)
Viren ermöglichen die Entwicklung individueller Schadsoftware und automatisieren Cyberangriffe. Sie gelangen beispielsweise durch einen Download in Ihr System.

PHISING
Ziel des Phising ist es, möglichst viele sensible Daten in kurzer Zeit zu erhalten. Mit Links in gefälschten Mails werden Sie z.B. zu fingierten Zahldiensten weitergeleitet. Dort geben viele Opfer nichtsahnend ihre persönlichen Daten an.

DENIAL-OF-SERVICE-ATTACKEN (DOS)
Hier wird ein Webserver oder ein Internetdienst so ausgelastet, dass er im Internet nicht mehr erreichbar ist. Diese Attacken werden oft als Ablenkungsmanöver eingesetzt um eine Schadsoftware zu aktivieren.

PHYSISCHER VERLUST
Der Diebstahl eines dienstlichen Laptops oder Handys kann sich für ein Unternehmen als verheerend herausstellen. Auf solchen Geräten sind Geschäfts- und Privatinformationen gespeichert. Mögliche Kosten durch den Verlust: Benachrichtigungskosten der Kunden, Krisenmanagementkosten, Abwehrkosten, Cyber-Vandalismus.

DATENVERLUST
Die schlimmste Folge der Cyberangriffe ist der Verlust (z.B. Diebstahl oder Löschung) sensibler Daten. So können beispielsweise Onlineüberweisungen getätigt oder Kreditkarten missbraucht werden. Auch der Diebstahl interner und externer Geschäftsgeheimnisse (beispielsweise von Vertragsvereinbarungen oder von Entwicklungs- und Produktionsplänen …) kann ein Unternehmen schnell an den Rand der Existenz bringen.

BESTEHT BEI IHREN BETRIEBLICHEN VERSICHERUNGEN BEREITS SCHUTZ?

BETRIEBSHAFTPFLICHT
In der Betriebshaftpflichtversicherung sind lediglich die Ansprüche eines geschädigten Dritten, jedoch keine Eigenschäden, abgedeckt. Der Schutz erstreckt sich auf den Datenverlust, die Datenveränderung und die Datenschutzverletzung. Zudem leisten einige Versicherer auch, wenn der versicherte Unternehmer Persönlichkeits- und Namensrechte verletzt.

SACH- UND TECHNISCHE VERSICHERUNG
Hier werden die Kosten für die Wiederherstellung der Daten sowie der betriebsfertigen Programme erstattet.

VERTRAUENSSCHADEN POLICE
Die Vertrauensschadenpolice kommt meist für die IT- Forensik sowie für die Wiederherstellungskosten nach einem Hackerangriff auf.

KIDNAP & RANSOM (K&P)
Diese Form der Absicherung leistet bei Erpessung und Bedrohung. Belohnungen für mögliche Hinweise zur Erfassung der Erpesser sind ebenfalls Inhalt der Deckung.

… dieser Schutz reicht aber bei Weitem nicht aus!

So werden beispielsweise Eigenschäden, z.B. Kosten für die Wiederherstellung verlorener oder gestohlener Daten und den dadurch resultierenden Ertragsausfall durch die Unterbrechung des Geschäftsbetriebes, nur selten bis gar nicht übernommen!