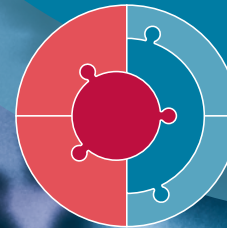


CYBER-VERSICHERUNG

Gewerbetreibende und Ärzte/Heilberufe

Cyber-Schutz, so individuell
wie die Unternehmen Ihrer
Kunden.



GESCHÄFTSPARTNER-
INFORMATION

Warum brauchen Unternehmen eine Cyber-Versicherung?

Wenn z. B. durch einen Hacker-Angriff Kundendaten entwendet und veröffentlicht wurden oder die Arbeitsfähigkeit beeinträchtigt wird, benötigt Ihr Kunde schnellstmöglich exzellente Hilfe und Unterstützung. Mit AL_CYBER kein Problem!

Welchen Schutz bietet die Cyber-Versicherung?

Versichert werden **Vermögensschäden** (keine Personen- oder Sachschäden) aufgrund einer **Informationssicherheitsverletzung**.



Wer Cyber-Attacken ausgesetzt ist, hat nicht nur den Schaden, sondern riskiert auch erhebliche Bußgelder bei Verstößen gegen die Datenschutz-Grundverordnung.

Eine Informationssicherheitsverletzung liegt in folgenden Fällen vor:

- Die elektronischen Daten oder informationsverarbeitenden-Systeme Ihres Kunden sind temporär oder dauerhaft nicht zugänglich. → Verfügbarkeit ist beeinträchtigt
- Die Daten sind nicht vollständig oder wurden verändert oder die korrekte Funktionsweise von Systemen ist nicht gewährleistet. → Integrität ist beeinträchtigt
- Die Daten werden Unberechtigten zugänglich gemacht. → Vertraulichkeit ist verletzt

Eine Informationssicherheitsverletzung wird durch folgende Ereignisse ausgelöst:

- Angriff oder unberechtigter Zugriff auf die elektronischen Daten Ihrer Kunden
- Angriff auf oder Eingriff in die IT-Systeme
- Schadprogramme wirken auf die elektronischen Daten oder IT-Systeme
- Eine Handlung oder Unterlassung führt zu einer Verletzung von datenschutzrechtlichen Vorschriften durch den Versicherungsnehmer



Welche Fälle wären abgesichert (Auszug)?

- Der Klassiker: Ein unachtsamer Klick im Internet und schon ist es passiert, die Daten werden verschlüsselt.
- Kriminelle erstellen täuschend echte Kopien von E-Mails (Phishing), um Zugangsdaten/Passwörter von Nutzern auszuspionieren.
- Ein unzufriedener Mitarbeiter will sich an der Firma rächen und schleust Schadsoftware ein.
- Ein Hacker bricht in die IT-Systeme ein und löscht, beschädigt, blockiert oder kopiert Daten.
- Die Website des Unternehmens wird gekapert.
- Eine DoS- oder DDoS-Attacke legt den Online-Shop lahm.
- Ein Computervirus/-wurm, Trojaner oder andere Schadsoftware beeinträchtigen die elektronischen Daten oder IT-Systeme. Betriebsunterbrechungen oder Datenschutz-Lecks sind die Folge.

Fakt



72% der Unternehmen schätzen das Risiko von Cyberkriminalität für den eigenen Betrieb als gering ein.

Aber: Von mehr als jedem zweiten Unternehmen waren Daten im Darknet zu finden, insbesondere E-Mail-/Passwort-Kombinationen

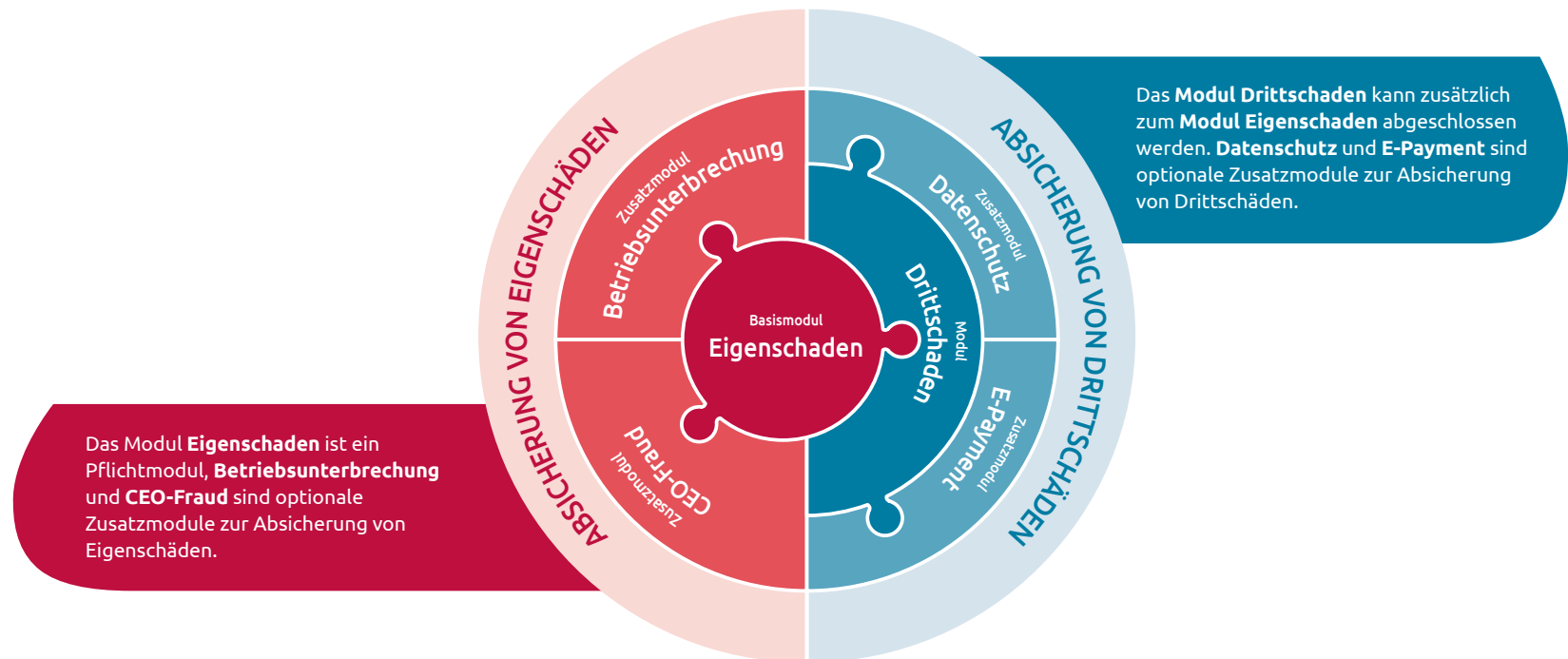
Quelle: GDV-Branchenreport Cyberrisiken im Mittelstand 2020

Die Vorteile des Modulbaukastens.

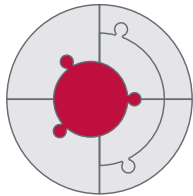
Sie können pro Modul eine eigene Deckungssumme und Selbstbeteiligung festlegen. Dies sorgt für einen bedarfsgerechten Schutz und reduziert damit Ihre Maklerhaftung. Um Ihnen die Ausgestaltung des Versicherungsschutzes zu erleichtern, haben wir Ihnen auf den folgenden Seiten einige Tipps zusammengefasst.

Weitere Besonderheiten und Highlights

- **Deckungssummen bereits ab 10.000 € möglich**, dies führt zu günstigen Einstiegsprämien
- **Transparent formulierte Obliegenheiten**
- Einfache Berechnung bei **Ärzten/Heilberufen anhand der Personenzahl**
- EC-/Kreditkarten-Monitoring
- CEO-Fraud (sog. „Fake President“)
- Elektronischer Zahlungsverkehr
- Vertragliche Schadensersatzansprüche
- BU inkl. Mehrkosten und BU durch Cloud-Ausfall
- Innovationsklausel
- Generell keine Sublimits



Absicherung von Eigenschäden



Modul Eigenschaden

Basismodul

Wir erstatten u. a. die folgenden Kosten bzw. Aufwendungen:

- **IT-Forensik/Schadenfeststellungskosten**
 - Kosten für die Ursachenermittlung und Feststellung des versicherten Schadens
 - Kosten des Versicherungsnehmers für externe Sachverständige und Mehrkosten durch den unterstützenden Einsatz von Mitarbeitern des VN
- **Datenwiederherstellung** (gilt auch für Software und Programme) sowie Entfernung der Schadsoftware
- **Sicherheitsverbesserungen nach einem Angriff**
Honorare von beauftragten Sicherheitsberatern einschließlich der Kosten für angemessene Sicherheitsverbesserungen, wenn diese Maßnahmen geeignet sind, einen zukünftigen Angriff zu verhindern
- **Kosten für Krisenkommunikation und PR-Maßnahmen**
zur Wiederherstellung der öffentlichen Reputation, z. B. durch Krisenmanager
- **Abwehr einer Cyber-Bedrohung/-Erpressung**
 - Kosten für Abwendung der Bedrohungslage durch einen von der Alte Leipziger zu benennenden und zu beauftragenden IT-Dienstleister
 - Kosten für Krisenberatung und -management
- **EC-/Kreditkarten-Monitoring-Service**



IT-Forensik

Die IT-Forensik beschäftigt sich mit der Analyse von tatsächlichen oder vermuteten Vorfällen im Zusammenhang mit IT-Systemen, um Sachverhalte, Ursachen und Verursacher festzustellen.

- **Elektronischer Zahlungsverkehr**
Übernahme der Verluste durch falsch ausgeführte, umgeleitete oder manipulierte Überweisungen
- **Aufwendungen vor Eintritt des Versicherungsfalls**
- **Schadenminderungskosten**
Aufwendungen des Versicherungsnehmers zur Minderung einer versicherten Betriebsunterbrechung oder zur Minderung eines sonstigen Schadens – unabhängig davon, ob der Versicherungsnehmer damit erfolgreich war oder nicht



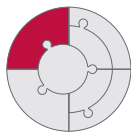
Beispiel Phishing-Mail: Ein Mitarbeiter öffnet den Anhang einer E-Mail und aktiviert einen Trojaner. Damit gelingt es einem Hacker, sich Zugang zu vertraulichen Kundendaten zu verschaffen und diese zu veröffentlichen. In diesem Fall übernehmen wir neben den Kosten für die Entfernung der Schadsoftware auch die notwendigen und angemessenen Honorare, Gebühren und Auslagen eines Krisenmanagers sowie Kosten für PR-Maßnahmen, um das Image wiederherzustellen.

Eigenschaden: Festlegung der Deckungssumme



Bei der Festlegung der Deckungssumme sollten – je nach Risikoeinschätzung – u. a. folgende Punkte berücksichtigt werden:

- Die Höhe der Kosten für die Wiederherstellung von Betriebssystemen, Datenbanken oder Verwaltungssystemen
- Die Kosten für einen IT-Dienstleister liegen durchschnittlich bei rund 300 € pro Stunde, sein Einsatz kann mehrere Tage dauern
- Die Höhe der Kosten für die Beauftragung eines Krisenmanagement- oder PR-Beraters



Zusatzmodul Betriebsunterbrechung optional

- Gesamter Zeitraum der **Betriebsunterbrechung** ist abgesichert
- Unabhängig davon, ob ein versicherter Cyber-Schaden im eigenen Betrieb oder bei einem entgeltlich beanspruchten Cloud-Anbieter zu einer Betriebsunterbrechung beim VN führt
- **Entgangener Betriebsgewinn und fortlaufende Kosten** werden erstattet
- Mitversichert sind auch Mehrkosten, die für die **Fortführung des Betriebes** aufgewendet werden müssen, z. B. Nutzung fremder IT-Systeme

Betriebsunterbrechung: Festlegung der Deckungssumme



Die Deckungssumme für das Zusatzmodul Betriebsunterbrechung errechnet sich durch Tagessatz x Haftzeit und wird im Online-Rechner automatisch ermittelt. Der Tagessatz ist 1/365 der Summe aus Vorjahresgewinn und jährlich fortlaufenden Kosten. Er kann in 50 €-Schritten (max. 5.000 €) gewählt werden. Mit der Haftzeit wählen Sie den Zeitraum, für den Versicherungsschutz besteht. Es sollte also berücksichtigt werden, wie viel Zeit für die Wiederherstellung der IT-Systeme im Höchstfall benötigt wird. Sie kann in 30-Tage-Schritten (max. 180 Tage) gewählt werden.



Hinweis

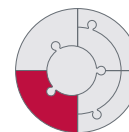
Sensibilisieren Sie Ihre Kunden für das Thema Datensicherung (Back-ups). Je besser und öfter die Daten gesichert wurden, desto reibungsloser und schneller funktioniert die Datenwiederherstellung.



Fakt

$\frac{2}{3}$ der Unternehmen haben Tage gebraucht, bis die IT-Systeme wiederhergestellt und die Schadsoftware beseitigt war.*

* Quelle: Forsa-Befragung Frühjahr 2020, Cyberrisiken im Mittelstand



Zusatzmodul CEO-Fraud optional

Erstattung missbräuchlich entwendeter Geldbeträge, die durch eine Vertrauensperson ausgezahlt wurden, weil ein unbefugter Dritter sich als Geschäftsführung ausgegeben hat und die Vertrauensperson zu dieser Zahlung angewiesen hat.

CEO-Fraud: Festlegung der Deckungssumme



Eine Orientierungshilfe für die Festlegung der Deckungssumme kann die Höhe etwaiger Zahlungsvollmachten für Mitarbeiter sein, bei denen die Zahlungsanweisungen nicht durch einen Vorgesetzten freigegeben werden müssen.

Cyber-Erpressung

Warum kein Lösegeld gezahlt werden sollte

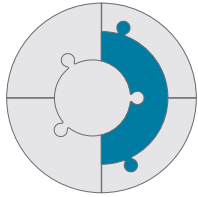
Erfahrungen zeigen: Wer einmal Lösegeld gezahlt hat, steht schnell auf einer „Kundenliste“ im Darknet, wird als „zahlungswillig“ und „erpressbar“ gekennzeichnet und ist anschließend weiteren Zahlungsforderungen und häufiger neuen Angriffen ausgeliefert.

Außerdem bedeutet eine Lösegeldzahlung noch lange nicht, dass die verschlüsselten Daten auch tatsächlich wieder entschlüsselt werden, denn einen entsprechenden Entschlüsselungs-Code gibt es meist gar nicht. Und die Schadsoftware wird mit einer Zahlung auch nicht entfernt. Bei einer Cyber-Erpressung im Zusammenhang mit einem Datendiebstahl und der Androhung einer Veröffentlichung der Daten bringt eine Lösegeldzahlung ohnehin nichts, da diese Daten auch weiterhin gestohlen bleiben. Deshalb raten auch das BKA und die Polizei ausdrücklich davon ab, dieses „Geschäftsmodell“ von Kriminellen zu unterstützen.

Was wird tatsächlich benötigt?

Nicht die Zahlung eines Lösegeldes! Sondern professionelle und schnelle Unterstützung: Die Schadsoftware muss entfernt, alle betroffenen Systeme müssen bereinigt und die Originaldaten müssen wiederhergestellt werden. Mit unserem Partner für Cyber-Security bieten wir genau diese Unterstützung, sodass der entstandene Schaden nicht die Existenz Ihrer Kunden bedroht, aber gleichzeitig auch deren Autonomie gestärkt wird.

Absicherung von Drittschäden



Modul Drittschaden

optionaler Schutz für Haftpflichtschäden

Dieses optionale Modul bietet Versicherungsschutz für den Fall, dass Ihr Kunde wegen einer Informationssicherheitsverletzung von einem Dritten auf Schadensersatz in Anspruch genommen wird.

- **Gegenstand der Haftpflicht**

Ansprüche aufgrund gesetzlicher Haftpflichtbestimmungen privatrechtlichen Inhalts



Beispiel Drittschaden: Ein Unternehmen stellt eine Datei für Kunden zum Download bereit, die unbeabsichtigt mit einem Computervirus infiziert ist.

Drittschaden: Festlegung der Deckungssumme



Bei der Festlegung der Deckungssumme für das Modul Drittschaden sollten die Ausrichtung des Unternehmens sowie die Art und Anzahl der verarbeiteten oder gespeicherten Daten (z. B. Kundendaten) berücksichtigt werden. Sofern vertragliche Schadenersatzansprüche mitversichert werden sollen, sind diese ebenfalls zu berücksichtigen.



Fakt

58% aller erfolgreichen Angriffe treffen über das E-Mail-Postfach ins Ziel.*

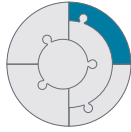
* Quelle: Forsa-Befragung Frühjahr 2020, Cyberisiken im Mittelstand

- **Rechtswidrige elektronische Kommunikation**

Ihr Kunde hat elektronische Medieninhalte veröffentlicht, die zu Persönlichkeitsrechts-, Namensrechts-, Urheberrechts- oder Markenrechtsverletzungen (und daraus resultierenden Verstößen gegen das Wettbewerbsrecht) führen.

Innerhalb dieses Moduls wählbar

Versicherungsschutz bei **vertraglichen Schadenersatzansprüchen** (Ansprüche wegen vergeblicher Aufwendungen im Vertrauen auf ordnungsgemäße Vertragserfüllung sowie Mehraufwendungen wegen Verzögerung der Leistung)



Zusatzmodul Datenschutz optional

Nach der aktuellen Rechtslage im Bereich Datenschutz sind Unternehmen, die Ziel einer Cyber-Attacke waren, bei denen also beispielsweise Daten von Kunden gestohlen oder von Unbefugten eingesehen wurden, verpflichtet, die Aufsichtsbehörde innerhalb von 72 Stunden umfassend zu informieren. Unabhängig von den Informationspflichten kann das attackierte Unternehmen auch Schadenersatzpflichtig gegenüber Dritten, z. B. Kunden, werden.

Das Zusatzmodul Datenschutz gibt Kostensicherheit

- für Schadenersatzansprüche Dritter, die gegen den Versicherungsnehmer aufgrund einer Datenschutzrechtsverletzung geltend gemacht werden,
- für die Rechtsberatung zu Informationspflichten,
- für die Benachrichtigung betroffener Dateninhaber (z. B. Kunden),
- für die Beauftragung eines externen Callcenters zur Beantwortung von Rückfragen.

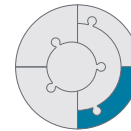
Datenschutz: Festlegung der Deckungssumme



Neben dem möglichen zu leistenden Schadenersatz sollten auch die Kosten für die rechtsanwaltliche Beratung bei einem Datenschutzvorfall (ca. 250 € bis 400 € pro Stunde) und für die Benachrichtigung betroffener Kunden (ca. 2,50 € pro Kundendatensatz) berücksichtigt werden.



Beispiel Hacker-Angriff: Unbekannte Täter hacken sich in die Systeme einer großen Arztpraxis und stehlen sensible Patientendaten. In diesem Fall übernehmen wir nicht nur die Kosten für die IT-Forensik zur Identifikation der betroffenen Patienten, sondern auch das Anwaltshonorar für die Beratung über die Informationspflichten sowie die Kosten für die Information der betroffenen Dateninhaber über den Diebstahl der Daten.



Zusatzmodul E-Payment optional

Versicherungsschutz für Forderungen zur Zahlung von Vertragsstrafen, die ein E-Payment-Serviceprovider wegen einer Verletzung eines „Payment Card Industry (PCI)“-Datensicherheitsstandards geltend macht.

E-Payment: Festlegung der Deckungssumme



Neben der möglichen Vertragsstrafe gemäß Strafenkatalog des E-Payment-Serviceproviders sollten hier auch 10 € je gespeichertem Kreditkartendatensatz berücksichtigt werden.

Soforthilfe im Notfall!



Cyber-Attacken sind Notfallsituationen, bei denen schnell gehandelt werden muss.

Ist der Versicherungsnehmer in einer Notfallsituation übernimmt die Alte Leipziger die Kosten eines Dienstleisters für die erste telefonische Notfall- und Krisenunterstützung in Form von:

- einer Experteneinschätzung zur geschilderten Lage,
- Empfehlungen für Sofortmaßnahmen zur Schadenbegrenzung,
- Empfehlungen für Sofortmaßnahmen zur Ursachenermittlung,
- einer ersten Bewertung der bisherigen Maßnahmen,
- ersten technischen Sofortmaßnahmen (sofern möglich/erforderlich).

Für die Soforthilfe fällt weder eine Selbstbeteiligung an noch werden diese Kosten auf die Deckungssumme angerechnet. Dies gilt jedoch nur, sofern der VN die Notfallsituation über die dem Versicherungsschein beigelegte Telefonnummer für die Cyber-Soforthilfe meldet und somit der vom Versicherer beauftragte Dienstleister die telefonische Soforthilfe durchführt.

Anhaltspunkte für eine Notfallsituation:

- Die Antivirensoftware oder die Firewall melden eine Infektion der IT-Systeme.
- Die Antivirensoftware oder die Firewall weisen Auffälligkeiten in den Logdateien auf.

Informationen zum Thema Prävention

Unser Cyber-Security-Dienstleister bietet Ihren Kunden zusätzlich auch Unterstützung bei der Schadensprävention, z. B.:

- Feststellung der aktuellen IT-Sicherheit
- Schwachstellen lokalisieren und beheben
- weitere Präventionsmaßnahmen wie z. B. Angriffssimulationen oder Mitarbeiterschulungen
- TÜV-Zertifizierungen



Hinweis

Cyber-Hotline rund um die Uhr (24/7) zur Meldung von eingetretenen, bevorstehenden oder vermuteten Schadenfällen:

 **06171 66-2206**

Einfach online abschließen.

Die Antragstellung geht ganz einfach über unseren Online-Rechner E@SY WEB Sach. Es gibt wenige Risikofragen und die Obliegenheiten haben wir mit leicht verständlichen Erläuterungen ergänzt.



Hier AL_CYBER einfach online abschließen:
www.al-rechner.de/cyber



Hinweis:

Weitere wichtige Fachbegriffe aus dem Cyber-Umfeld finden Sie hier in unserem Glossar: www.vermittlerportal.de/glossar-cyber-fhs081.pdf

Wie wird die Prämie ermittelt?

Maßgeblich für die Prämie sind neben den Risikomerkmalen – wie z. B. die ausgeführte Tätigkeit, der Umsatz, die Anzahl und Art der verarbeiteten Daten und die IT-Durchdringung des Unternehmens – auch der gewählte Deckungsumfang, also Module, Deckungssummen und Selbstbeteiligungen. Daher lässt sich an dieser Stelle keine Faustformel ableiten.

Um Ihnen die Festlegung des Deckungsumfangs zu erleichtern, finden Sie im Online-Rechner zu jedem Modul Infotexte.

Besonderheit bei Zielgruppe Ärzte/Heilberufe

Diese wird nach Personen berechnet, dadurch erhalten Sie schnell bzw. mittels sehr weniger Informationen eine Prämie.

Obliegenheiten: Transparent formuliert

Bei Vertragsabschluss ist zu bestätigen, dass die erforderlichen Voraussetzungen in Bezug auf die IT-Sicherheit vorhanden sind.

Hierzu zählen u.a.:

- Individuelle und mit einem Passwort gesicherte Zugänge für alle Nutzer der IT
- Schutz der IT mit einer Firewall gegen unberechtigten Zugriff
- Verschlüsselter Datenversand
- Schutz vor Schadsoftware (z. B. Antivirenprogramm)
- Regelmäßige Sicherheitsupdates
- Mindestens wöchentliche Datensicherung (Sicherungsdatenträger physisch getrennt von den Originaldaten aufbewahren)
- Einhaltung aller gesetzlichen, behördlichen sowie vertraglich vereinbarten Sicherheitsvorschriften

Hierbei handelt es sich um Kurzbeschreibungen. Den rechtsverbindlichen Wortlaut, nähere Erläuterungen und Empfehlungen zu den Obliegenheiten enthält das Dokument C 02. Dieses und alle weiteren Druckstücke finden Sie im Vermittlerportal und im Online-Rechner.

Weltweiter Versicherungsschutz



Dies gilt, soweit die Ansprüche in EWR-Staaten und nach deren Recht geltend gemacht werden. Für Betriebsstätten und IT-Systeme (z. B. Server, Produktions- oder Vertriebsniederlassungen, Lager), die vom Kunden selbst betrieben werden, besteht Versicherungsschutz ausschließlich innerhalb der Bundesrepublik Deutschland.

Haben wir Sie von unserer AL_Cyber überzeugt?

Weitere Informationen finden Sie in unserem
Vermittlerportal, wie beispielsweise

- Erklärfilm
- Broschüre mit Schadenbeispielen
- Broschüre für Endkunden
- Online-Cyber-Rechner

Nehmen Sie gerne Kontakt mit einem regionalen
Ansprechpartner auf und erfahren Sie noch mehr.
Ihren Ansprechpartner finden Sie unter:
www.vermittlerportal.de/sach/kontakt-neu-anbindung

Folgen Sie uns



Alte Leipziger

Versicherung AG
Alte Leipziger-Platz 1
61440 Oberursel
sach@alte-leipziger.de
www.vermittlerportal.de

Ihr Experte vor Ort: