Allianz Elementar Versicherungs-AG

Allianz Business & Allianz Cyber-Schutz

Informationsunterlage

Allianz

Die Inhalte dieser Unterlage wurden mit größtmöglicher Sorgfalt zusammengestellt, dennoch übernimmt die Allianz keine Haftung für die Richtigkeit, Vollständigkeit und Aktualität der enthaltenen Informationen.

Aus dieser Unterlage können keine Rechtsansprüche – gleichgültig welcher Art – abgeleitet werden.

Die Allianz ist bemüht, die in dieser Unterlage enthaltenen Informationen, insbesondere bei Vorliegen eines Bedarfs, zu aktualisieren, jedoch übernimmt sie hierfür keine Verpflichtung.

Regelungen bezüglich der Selbstbehalte finden sich in den Allgemeinen, Ergänzenden Allgemeinen und Besonderen Versicherungsbedingungen.
Der angeführte Leistungsumfang stellt einen Auszug aus den Allgemeinen, Ergänzenden Allgemeinen und Besonderen Versicherungsbedingungen dar. Diese werden dadurch nicht ersetzt. Vollständige Informationen entnehmen Sie bitte dem Antrag, der Versicherungsurkunde und den jeweiligen Versicherungsbedingungen.

Bei allen personenbezogenen Bezeichnungen (z.B. Versicherungsnehmer, Vertragspartner, Sachverständiger, etc.) gilt die gewählte Bezeichnung für beide Geschlechter.

Änderungen, Irrtümer und Druckfehler vorbehalten.
Stand der Informationen Juni 2017

Allianz Elementar Versicherungs-Aktiengesellschaft,
Sitz: 1130 Wien, Hietzinger Kai 101–105
Telefon: 05 9009-0, Telefax: 05 9009-70000
Eingetragen im Firmenbuch des Handelsgerichts Wien
unter FN 34004g, UID: ATU 1536 4406, DVR: 0003565
Internet: http://www.allianz.at

Aufsichtsbehörde:
Finanzmarktaufsicht, 1090 Wien, Otto-Wagner-Platz 5, www.fma.gv.at

Inhalt

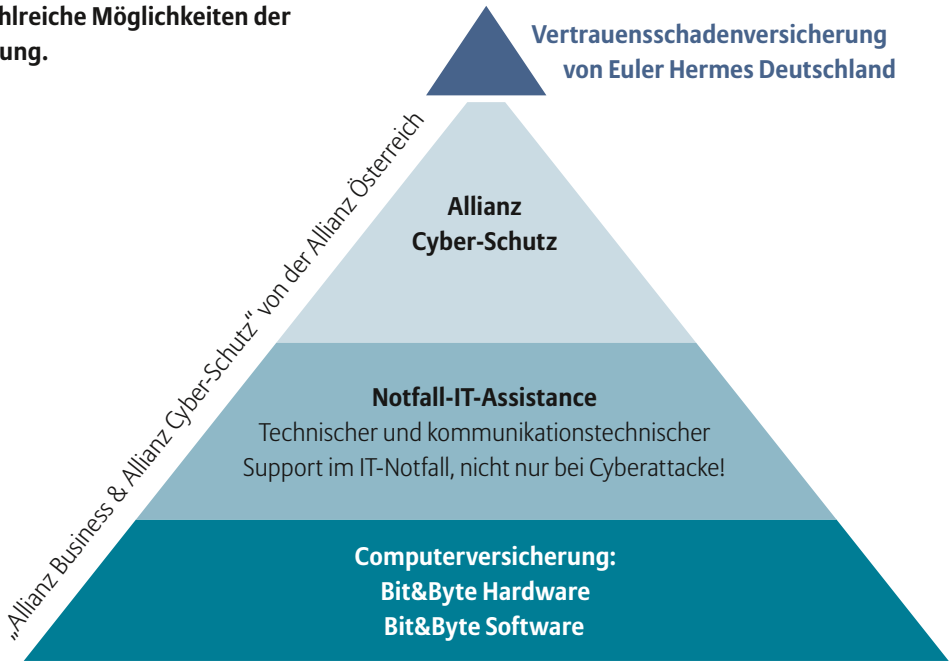
Allgemeines

Computer, Laptop oder Netzwerke sind aus der Arbeitswelt nicht mehr wegzudenken.

Schäden im Bereich der Informationstechnologie häufen sich. Geräte werden plötzlich und unerwartet kaputt. Derartige technische Probleme verlangen nach rascher Hilfe. Cyber-Attacken und Datenverlust können massiv ins Geld gehen.

Jedes Modul (=Möglichkeit der Absicherung) kann auch einzeln abgeschlossen werden. Der modulare Aufbau ermöglicht ein an das Unternehmen angepasstes Absicherungskonzept.

„Allianz Business" mit „Allianz Cyber-Schutz" bietet zahlreiche Möglichkeiten der Absicherung.



Diese Informationsunterlage ermöglicht einen ausführlicheren Überblick über "Allianz Business & Allianz Cyber-Schutz".

Wichtig:

Es gehört zur unternehmerischen Sorgfaltspflicht, dass unverzüglich

- die entsprechenden Updates des Betriebssystems
- die entsprechenden Updates der verwendeten Programme
- die entsprechenden Updates der Virenschutzprogramme

durchgeführt werden.

Es gehört zur unternehmerischen Sorgfaltspflicht, dass die Firewall installiert und gewartet ist.

Es gehört zur unternehmerischen Sorgfaltspflicht, dass Programme und Daten entsprechend gesichert und Passwörter regelmäßig geändert werden.

Computerversicherung Bit&Byte Hardware

Im Rahmen der Computerversicherung können stationäre Hardware (z.B. der Informationstechnik und/oder der Kommunikationstechnik), ebenso wie mobile Büro- und EDV-Geräte versichert werden.

Was ist versichert?

Versicherungsschutz besteht für die versicherte Hardware gegen plötzlich und unvorhergesehen eintretende Beschädigung oder Zerstörung (Sachschaden) sowie bei Verlust durch Einbruchdiebstahl, Diebstahl oder Raub.

Als Sachschaden gilt eine nachteilige Veränderung der Sachsubstanz.

Folgende stationäre Geräte können – wenn sie im Betrieb verwendet werden – mit einer Pauschalversicherungssumme zum Neuwert versichert werden:

- stationäre Informationstechnik (inkl. CAD- und CAM-Computer, Computerkassen),
- stationäre Kommunikationstechnik (inkl. Videokonferenz-, Gegen- und Wechselsprechanlagen),
- stationäre Bürotechnik (inkl. Registrierkassen, Küchengeräte im Büro),
- stationäre Sicherungs- und Meldetechnik (inkl. Zutrittskontrollanlagen, Signalanlagen).

Bei der Allianz können auch mobile Büro- und EDV-Geräte mit einer Pauschalversicherungssumme zum Neuwert versichert werden. Der Geltungsbereich dieser Hardware-Versicherung ist weltweit!

Was leistet die Allianz im Versicherungsfall?

Der Versicherer ersetzt im Rahmen der Versicherungssumme

- bei Zerstörung oder Verlust den Versicherungswert der vom Schaden betroffenen Sache unmittelbar vor Eintritt des Schadenereignisses (Neuwert),
- bei Beschädigung die notwendigen Reparaturkosten zur Zeit des Eintritts des Schadenereignisses (Neuwert).

War der Zeitwert der vom Schaden betroffenen Sache unmittelbar vor Eintritt des Schadenereignisses kleiner als 40 % des Neuwerts, wird höchstens der Zeitwert ersetzt.

Mitversicherbar sind Mehrkosten infolge Technologiefortschritt: Dies bedeutet, falls es bei Zerstörung oder Verlust keine Möglichkeit der Wiederbeschaffung gleichwertiger Ersatzgeräte (gleicher Art und Güte) gibt, ersetzt der Versicherer den Neuwert plus max. 20 % des Neuwerts, jedoch maximiert mit € 10.000,–.

Mögliches Beispiel:
Auf dem Heimweg wurde dem Unternehmer seine Umhängetasche samt Firmenlaptop und Beamer geraubt. Die Beschaffungskosten betrugen € 4.345,–.

Bit&Byte Office – Mehrkosten-Versicherung

Was ist versichert?

Versicherungsschutz besteht bei gänzlicher oder teilweiser Betriebsunterbrechung, wenn die versicherte Hardware infolge eines versicherten Schadens stillsteht.

Was leistet der Versicherer im Versicherungsfall?

Der Versicherer ersetzt innerhalb der versicherten Haftungszeit die Mehrkosten, die für die Weiterführung der Betriebstätigkeit aufgewendet werden müssen (zum Beispiel Anmietung fremder Hardware).

Computerversicherung Bit&Byte Software

Zusätzlich zur Hardware kann auch die Software (Daten und Programme) versichert werden.

Mitversichert sind bei der Bit&Byte Software auch die externen, ihrer Bestimmung nach auswechselbaren, Datenträger (zur Sicherung notwendige Datenspeicher) und die auf diesen befindlichen Daten und Programme (maschinenlesbare Informationen).

Was ist versichert?

Versichert gelten nachteilige Veränderungen oder Verluste von versicherten Daten und Programmen infolge eines versicherten Sachschadens an der Hardware oder durch

- Störung oder Ausfall der Datenverarbeitungsanlage oder der Klimaanlage,
- Bedienungsfehler (zum Beispiel falscher Einsatz von Datenträgern, falsche Befehlseingabe),
- Über- oder Unterspannung,
- elektrostatische Aufladung, elektromagnetische Störung,
- höhere Gewalt (einschließlich Blitzeinwirkung),
- Schäden an elektronischen Bauelementen (Bauteile),
- Schäden an Sicherungselementen aller Art durch ihre bestimmungsgemäße Funktion.

Was leistet der Versicherer im Versicherungsfall?

Der Versicherer ersetzt im Rahmen der Versicherungssumme die notwendigen Kosten für erforderliche

- Wiederherstellung bzw. Wiederbeschaffung von versicherten externen Datenträger (zur Sicherung notwendige Datenspeicher),
- Wiederbeschaffung und Wiedereingabe der Daten und Programme für den, vor Eintritt des Schadenfalles, befindlichen Zustandes des Betriebssystems und der Programme,
- Wiederaufbringung bzw. maschinelle Wiedereingabe der versicherten Daten und Programme aus externen Datenträgern (zur Sicherung notwendige Datenspeicher),
- maschinelle oder manuelle Wiedereingabe der Daten aus Ursprungsprogrammen oder aus beim Versicherungsnehmer vorhandenen Belegen, einschließlich deren Zusammenstellung und Aufbereitung.

Beispiel:

Durch einen Bedienungsfehler (falsche Befehlseingabe) gingen die Buchungsdaten des letzten Arbeitstages verloren, die Wiederherstellung der Daten kostet € 2.500,–.

Notfall-IT-Assistance

Wenn es plötzlich und unvorhergesehen zu einem Systemausfall der Hardware und/oder der Betriebssysteme kommt, dann ist rasche Hilfe (rund um die Uhr – 365 Tage) notwendig.

Was ist ein IT-Notfall und was wird geleistet?

IT-Notfälle mit Systemausfall

Als IT-Notfall gilt, wenn es plötzlich und nicht vorhersehbar zu einem Systemausfall der Hardware (Laptops, PCs, Netzwerke, ausgenommen Registrierkassen) und/oder der Software (Betriebssystem) kommt durch

- Cyber-Angriffe oder Verdacht auf diese,
- technischen Defekt der Hardware (Laptop und PC), fehlerhafte Bedienung der Hard- und/oder Software (Betriebssystem),
- nachteilige Veränderungen oder Verluste von für den Betrieb wichtigen Daten und Programme durch Schad-Software. Der Begriff Schad-Software umfasst zum Beispiel Viren, Trojaner, Würmer und Zeit- oder Logikbomben.

IT-Notfälle ohne Systemausfall

- Befall von Schad-Software (zum Beispiel Viren, Trojaner, …),
- Cyber-Erpressung (zum Beispiel Ransomware, PC-Blockade, …),
- Rufschädigung (zum Beispiel Mobbing, unerlaubte Veröffentlichung von Fotos, …),
- Unberechtigte Abmahnung (zum Beispiel „free" Downloads, …),
- Identitätsdiebstahl (zum Beispiel ID Theft, falsche Bestellung, …),
- E-Mail-Betrug (zum Beispiel falsche Gewinne, Geldtransfer etc.), inklusive Phishing,
- Gefälschte Webseiten, inklusive Pharming,
- Verlust persönlicher Daten (zum Beispiel Spyware etc.),
- Denial of Service.

Was wird im IT-Notfall geleistet?

Im Falle eines IT-Notfalls werden von der Assistance-Zentrale hierfür qualifizierte Personen am Telefon zur Verfügung gestellt, die in Absprache mit dem Geschäftsführer bzw. dem Firmeninhaber den IT-Notfall lösen (rund um die Uhr – 365 Tage).

Im IT-Notfall kann es zur Problemlösung notwendig sein, dass – wenn vom Versicherungsnehmer erlaubt – sich ein Spezialist mit dem System des Versicherungsnehmers verbinden muss.

In seltenen IT-Notfällen kann es notwendig sein, dass ein Experte in den Betrieb des Versicherungsnehmers kommen muss. In solchen Fällen wird – wenn vom Versicherungsnehmer gewünscht – von der Assistance-Zentrale ein Experte organisiert. Einmal pro Jahr werden die Kosten für eine einmalige An- und Abreise sowie eine Arbeitsstunde übernommen.

Was ist ein Kommunikations-Notfall und was wird bei einem Kommunikations-Notfall geleistet?

Als Kommunikations-Notfall gilt, wenn ein plötzlicher und nicht vorhersehbarer Kommunikationsbedarf im Zusammenhang

- mit einem IT-Notfall besteht.
- mit einer existenzbedrohenden Krise aufgrund von Vorwürfen in Medien aller Art besteht. Eine existenzbedrohende Krise ist ein plötzliches und unerwartetes Ereignis, das den Fortbestand des Versicherungsnehmers massiv gefährdet.

Was wird im Falle eines Kommunikations-Notfalls geleistet?

Im Falle eines Kommunikations-Notfalls werden von der Assistance-Zentrale (rund um die Uhr – 365 Tage) hierfür qualifizierte Personen bereitgestellt (z.B. PR-Berater, Consultant), die in Absprache mit dem Geschäftsführer bzw. dem Firmeninhaber Lösungswege vorschlagen und eine Medienbetreuung durchführen (zum Beispiel Info an Zeitungen, Fernsehen, Geschäftspartner etc.). Im Versicherungsfall werden Leistungen in Summe bis max. € 2.500,– erbracht.

Weitere Dienstleistungen, die angeboten werden (rund um die Uhr – 365 Tage):

Vermittlung von Ersatz-Hard- und/oder Software

Bei einer Zerstörung, Beschädigung oder bei Abhandenkommen der für den Betrieb des Versicherungsnehmers unbedingt notwendigen Hard- und/oder Software hilft die Assistance-Zentrale, je nach Verfügbarkeit und Möglichkeit, bei der Organisation eines entsprechenden Ersatzes. Die Kosten für Hard- und/oder Software hat der Versicherungsnehmer selbst zu tragen.

Vermittlung von Spezialisten

Bei Bedarf (unabhängig vom Schadenereignis) hilft die Assistance-Zentrale, je nach Verfügbarkeit und Möglichkeit, bei der Organisation eines Termins bei einer IT-Sicherheitsfirma und/oder Datenschutzspezialisten. Die Kosten für die Spezialisten hat der Versicherungsnehmer selbst zu tragen.

Beispiel:

Herr A betreibt eine Kfz-Werkstätte. Als Kunde B die Werkstatt betritt und die Sekretärin diesen Kunden in der Kundenverwaltung aufrufen will, geht nichts mehr. Der Bildschirm ist schwarz. Die üblichen Ursachen „kein Strom“, „Bildschirm nicht mit PC verbunden“ usw. sind schnell ausgeschlossen. Ein Telefonat mit der Assistance-Zentrale schafft Klarheit. Der Betrieb ist Opfer einer Cyber-Attacke geworden, und nach Installation der entsprechenden Sicherungen unter Anweisung des Experten geht alles wieder seinen Lauf. Kunde B postet inzwischen Beschimpfungen auf der Social Media-Seite der Kfz-Werkstätte. Auch hier hilft gleich die Kommunikations-Notfall-Assistance, formuliert die entsprechende Darstellung auf der Social Media-Seite und fordert den Kunden B auf, solche Meldungen zu unterlassen.

Hinweis: Begrenzung der Leistung

Keinesfalls übernommen werden

- Verluste aller Art (zum Beispiel Vermögensnachteile durch Falsch-Überweisung, finanzielle Schäden durch Handel oder Zahlungen),
- Kosten für neue Geräte bzw. Ersatzgeräte oder Ersatzteile,
- Kosten für die Neuanschaffung von Software,
- Kosten für die Wiederherstellung von Daten oder Software (zum Beispiel Neuprogrammierung oder Nacherfassung von Daten).

Allianz Cyber-Schutz

Der Allianz Cyber-Schutz bietet nicht nur Versicherungsschutz bei Cyber-Attacken, sondern auch wenn Daten verlorengehen.

Was ist versichert?

Versicherungsschutz für Haftpflichtansprüche

Unternehmen haften für Schäden, die sie selbst oder ihre Mitarbeiter Anderen durch die betriebliche Tätigkeit zufügen. Es kann möglicherweise zu Schadenersatzansprüchen kommen, damit verbunden sind oftmals sehr hohe Anwaltskosten, die das Unternehmen finanziell belasten.

Betreffend den Versicherungsschutz gilt das Claims made-Prinzip: beitragsfreie Rückwärtsdeckung von 6 Monaten (Versicherungsschutz für unbekannte Fehler aus der Vergangenheit, wenn diese Fehler erst während der Vertragslaufzeit erstmalig bekannt geworden sind und geltend gemacht werden).

Versichert sind:

- Schadenersatzansprüche wegen einer Datenschutz- oder einer Vertraulichkeitsverletzung
- Schadenersatzansprüche wegen unzureichender Netzwerksicherheit
- Schadenersatzansprüche wegen rechtswidriger digitaler Kommunikation (Marken- und Urheberrecht, Wettbewerbsrecht)
- Vertragsstrafe wegen Verletzung von Payment Card Industry Sicherheitsstandards

Die Versicherungssumme steht einmal pro Versicherungsfall zur Verfügung!

Versicherungsschutz für bestimmte Eigenschäden

Der Versicherungsfall im Falle einer Betriebsunterbrechung tritt ein mit der ersten Feststellung der teilweisen oder kompletten Nichtverfügbarkeit des Computersystems.

Im Rahmen der Versicherungssumme sind versichert die **Betriebsunterbrechung bis max. 3 Monate** durch die teilweise oder komplette Nichtverfügbarkeit des Computersystems aufgrund

- eines Cyber-Angriffs oder
- der Verfügung einer Datenschutzbehörde oder
- der Erfüllung einer gesetzlichen Verpflichtung eines Versicherten aufgrund einer Datenschutz- oder Vertraulichkeitsverletzung,

sowie der notwendige **Wiederherstellungsaufwand.**

Wiederherstellungsaufwand sind die entstandenen angemessenen Honorare, Auslagen und Aufwendungen für einen IT-Berater zum Zwecke der Wiederherstellung der versicherten Computersysteme. Dazu zählen auch die technische Wiederherstellung, Wiedergewinnung oder Neuinstallation von Daten oder Software, einschließlich der Kosten für den Erwerb einer Softwarelizenz, die zur Reproduktion der Daten oder der Software erforderlich ist.

Versicherungsschutz für Datenschutzverfahren

Der Versicherungsfall tritt mit dem erstmaligen Zugang einer schriftlichen Anzeige zur Einleitung des behördlichen Verfahrens ein.

Es besteht Versicherungsschutz bei **behördlichen Datenschutzverfahren** für die Abwehrkosten, wenn ein Straf-, Verwaltungsstrafverfahren oder sonstiges behördliches Verfahren wegen einer Datenschutz- oder einer Vertraulichkeitsverletzung eingeleitet wird.

Versicherungsschutz für Krisenmanagement

Forensische Dienstleistungen

Versicherungsschutz besteht im Rahmen der Versicherungssumme für forensische Dienstleistungen, um im Falle eines – durch tatsächliche Anhaltspunkte – begründeten Verdachts, dass

- eine Datenschutz- oder Vertraulichkeitsverletzung oder
- ein Cyber-Angriff

zu einem Schaden führen könnte, feststellen zu lassen, ob und in welchem Ausmaß eines der vorher genannten Ereignisse eingetreten ist, was die Ursache für den Eintritt war und welches die geeigneten Maßnahmen zur Schadenminderung sind.
Es werden in einem solchen Fall die angemessenen Honorare, Auslagen und Aufwendungen eines externen IT-Beraters ersetzt.

Krisenkommunikation

Versicherungsschutz besteht im Rahmen der Versicherungssumme für Krisenkommunikation im Fall

- einer Datenschutz- oder Vertraulichkeitsverletzung,
- eines Cyber Angriffs,
- der fehlerhafter Bedienung des Computersystems ,
- eines unvorhergesehenen technischen Problems des Computersystems,
- des Vorwurfs durch Medien einer Datenschutz- oder Vertraulichkeitsverletzung

zur Abwehr oder zur Minderung eines Schadens für das Ansehen.
In einem solchen Fall werden die angemessenen Honorare, Auslagen und Aufwendungen eines externen Beraters ersetzt.

Informationskosten

Versicherungsschutz besteht im Rahmen der Versicherungssumme für notwendige Informationskosten, die dem Versicherungsnehmer aufgrund einer behaupteten, tatsächlichen oder vermuteten Datenschutzverletzung oder einer behaupteten, tatsächlichen oder vermuteten Vertraulichkeitsverletzung entstehen.
Informationskosten sind die notwendigen und angemessenen Honorare, Auslagen und Aufwendungen für externe Beratung, welche dadurch entstehen, dass

- Daten auf dem Computersystem einer versicherten Gesellschaft ermittelt und gesichert werden;
- der Versicherungsnehmer sich über seine Rechtspflichten zur Anzeige der Datenschutzverletzung oder Vertraulichkeitsverletzung gegenüber Datenschutzbehörden, Dritten oder betroffenen Datensubjekten beraten lässt;
- der Versicherungsnehmer entsprechend seiner Rechtspflichten Anzeigen der Datenschutzverletzung oder Vertraulichkeitsverletzung gegenüber den maßgeblichen Datenschutzbehörden oder Dritten vornimmt.

Beispiele

- Herr B. leitet ein Outdoor-Geschäft mit einem eigenen Online-Shop, der rund 100.000 Kunden zählt. Als sein Kreditkartenunternehmen ihn auf Ungereimtheiten hinweist und eine Prüfung des Vorfalls verlangt, merkt Herr B., dass er das Opfer von Hackern geworden ist. Daraufhin kündigen die Behörden ein Datenschutz-Verfahren an. Herr B. muss den Onlinevertrieb vorerst einstellen. In Summe ein Schaden von € 150.000,–.

- Frau D. ist Geschäftsführerin eines Produktionsbetriebes. Nach einer Auseinandersetzung mit seinem Vorgesetzten ist ein Mitarbeiter so erbost, dass er das Unternehmen schädigen will. Er bleibt nach Dienstschluss heimlich im Betrieb, verschafft sich unberechtigten Zugang zu Daten für einen aktuellen Produktionsvorgang und zerstört diese. Am nächsten Tag steht nicht nur die eigene Produktion still, auch die Kunden des Unternehmens können nicht weiterarbeiten und machen ihren Produktionsausfall geltend.
  In Summe ein Schaden von € 2.000.000,–.

- Das Online-Buchungsportal eines Reisebüros wird durch eine Schadsoftware lahmgelegt. Der Angreifer verlangt Lösegeld zur Behebung des Problems. Das Problem kann mittels externen Spezialisten ohne Zahlung von Lösegeld behoben werden. Die Gesamtkosten für die Fehlersuche und Behebung, Datenwiederherstellung sowie Betriebsunterbrechung betragen € 1.100.000,–.

- Einbrecher stehlen mehrere Computer eines Handelsunternehmens, auf denen Kundendatensätze gespeichert sind. Es entstehen Kosten für IT-Forensik, Wiederherstellung der Daten, Beauftragung eines Rechtsanwalts und Information der betroffenen Kunden sowie der Datenschutzbehörde von insgesamt € 240.000,–.

Vertrauensschadenversicherung von Euler Hermes Deutschland

In der Vertrauensschadenversicherung ist der finanzielle Nachteil eines Unternehmens, der auf ganz bestimmte Sachverhalte zurückzuführen ist, versichert.

Was ist versichert?

Eingriffe Dritter in das EDV-System

Versicherungsschutz besteht für Vermögensschäden, die direkt dem versicherten Unternehmen durch vorsätzliche, rechtswidrige und zielgerichtete Eingriffe Dritter in das EDV-System des versicherten Unternehmens (Hackerschäden) zugefügt werden, soweit sich ein Dritter bereichert hat und der Dritte nach den gesetzlichen Bestimmungen zum Schadenersatz verpflichtet ist.

Vermögensschäden, die durch Dritte verursacht werden

Versicherungsschutz besteht für Vermögensschäden, die entstehen,

- wenn eine Vertrauensperson (zum Beispiel ein Mitarbeiter) gefälschte Wechsel, Schecks oder gesetzliche Zahlungsmittel eines Mitglieds des Europäischen Wirtschaftsraums (EWR), der USA oder Kanadas für das versicherte Unternehmen von einem Dritten entgegengenommen hat,
- wenn eine Vertrauensperson (zum Beispiel ein Mitarbeiter) aufgrund einer von einem Dritten gefälschten Anweisung, Bestellung oder Rechnung eine Zahlung oder Warenlieferung für das versicherte Unternehmen ausgeführt hat.

Vermögensschäden, die durch Verrat von Betriebs- und Geschäftsgeheimnissen durch Vertrauenspersonen entstehen

Versicherungsschutz besteht für Vermögensschäden, die direkt dem versicherten Unternehmen durch vorsätzliche unerlaubte Handlungen einer identifizierten Vertrauensperson (zum Beispiel Mitarbeiter) zugefügt werden, indem diese vorsätzlich und rechtswidrig dem versicherten Unternehmen gehörende Betriebs- und Geschäftsgeheimnisse

- an unberechtigte Dritte weitergibt,
- selbst missbräuchlich verwendet.

Vermögensschäden , die durch Vertrauenspersonen verursacht wurden

Versicherungsschutz besteht für Vermögensschäden,

- die dem versicherten Unternehmen von einer identifizierten Vertrauensperson (zum Beispiel Mitarbeiter) durch vorsätzliche unerlaubte Handlungen direkt zugefügt werden und die nach den gesetzlichen Bestimmungen die identifizierte Vertrauensperson zum Schadenersatz verpflichten,
- die eine identifizierte Vertrauensperson (zum Beispiel Mitarbeiter) durch vorsätzliche unerlaubte Handlungen einem Dritten unmittelbar zugefügt hat und das versicherte Unternehmen dem Dritten aufgrund einer vertraglichen oder gesetzlichen Verpflichtung zum Schadenersatz verpflichtet ist und die identifizierte Vertrauensperson zum Schadenersatz verpflichtet ist,
- auch wenn die Vertrauensperson nicht identifiziert werden kann, besteht Versicherungsschutz, wenn die unerlaubte Handlung, dem Tathergang nach, mit überwiegender Wahrscheinlichkeit von einer Vertrauensperson durchgeführt wurde.

Beispiele

- Ein Buchhalter veruntreut Gelder seines Arbeitgebers und überweist jahrelang kleinere Geldbeträge auf sein eigenes Konto. Um diese Aktionen zu vertuschen, manipuliert er die Datensätze der Buchhaltung. Als seine Machenschaften entdeckt werden, muss die Firma einen Verlust von über € 100.000,– feststellen. Die Vertrauensschadenversicherung kommt für den finanziellen Schaden des Unternehmens auf.

- Aufgrund eines Hacker-Angriffs bekommt die Buchhalterin ein gefaktes E-Mail des angeblichen Ge-

schäftsführers mit der Anweisung, dass sie rasch eine Anzahlung für ein Geschäft in Höhe von € 25.000,– auf ein bestimmtes Konto überweisen soll. Sie macht dies. Es stellt sich dann bei der Monatsprüfung heraus, dass das Unternehmen angegriffen wurde und mehrere gefälschte Rechnungen bezahlt wurden. Die Vertrauensschadenversicherung kommt für den finanziellen Schaden des Unternehmens auf.

- Ein Dritter hackt sich in die Telefonanlage des Versicherungsnehmers ein, um auf dieser Auslandsgespräche zu führen. Die Vertrauensschadenversicherung kommt für den finanziellen Schaden des Unternehmens auf.

- Ein Dritter schafft es durch manipulierte E-Mails oder Ausspähen („Phishing", „Spyware") an Benutzerdaten zu gelangen und veranlasst mehrere Überweisungen. Sofern die Bank keinen Ersatz leistet, kommt die Vertrauensschadenversicherung für den finanziellen Schaden des Unternehmens auf.

Hinweis:
Die Allianz Elementar Vers.-AG zeichnet keine Vertrauensschadenversicherung. Vertrauensschadenversicherung kann bei Euler Hermes Deutschland gezeichnet werden. Euler Hermes Deutschland ist kein Unternehmen der Allianz Gruppe Österreich.
Die Allianz Elementar Vers.-AG stellt dieses Produkt im Rahmen einer Marketing-Kooperation mit Euler Hermes Deutschland dar.
Nähere Informationen zu diesem Produkt finden Sie unter **www.eulerhermes.de**

Euler Hermes Deutschland
Niederlassung der Euler Hermes SA
22746 Hamburg
Hausanschrift:
Friedensallee 254, 22763 Hamburg
Tel. +49 (0) 40/88 34-0
Fax +49 (0) 40/88 34-77 44
E-Mail: info.de@eulerhermes.com

Information zum Thema IT-Sicherheit

Seitens der Wirtschaftskammer gibt es zahlreiche Möglichkeiten, sich als Unternehmer allgemein zum Thema IT zu informieren.

Informieren Sie sich bitte, zum Beispiel bei der Wirtschaftskammer auf

- **www.it-safe.wkoratgeber.at** (hier gibt es den Online-Ratgeber it-safe) **oder**
- **www.wko.at/site/it-safe/Sicherheitshandbuch.html** (hier gibt es das IT-Sicherheitshandbuch für KMUs zum Download oder zum Bestellen)

Dokumentieren Sie, dass Sie regelmäßig einen IT-Check machen!

Internet-Seiten mit weiteren interessanten Informationen

Meldestelle Cybercrime

Wenn Sie einen Verdacht auf Internetbetrug haben und über die weitere Vorgangsweise Informationen benötigen, wenden Sie sich bitte an folgende E-Mail-Adresse des Bundeskriminalamts:
against-cybercrime@bmi.gv.at

www.bmi.gv.at/cms/BK/meldestellen/internetkrimina/start.aspx

Betrugsformen im Internet

Auf dieser Seite des Bundeskriminalamts werden Sie über aktuelle Betrugsmaschen informiert und bekommen Tipps.

www.bmi.gv.at/cms/BK/betrug/start.aspx

Begriffsdefinitionen von A wie Adware bis W wie Whaling

(Stand April 2017)

Adware

Das Wort „Adware" ist eine Zusammensetzung aus den englischen Wörtern „advertising (=Werbung)" und „software". Adware ist also Software, die zu Werbezwecken eingesetzt wird. Meist gelangt Adware über heruntergeladene Programme auf den Rechner. Wenn beispielsweise ein Programm installiert wird und bei der Installation alle Komponenten zugelassen werden, kann auch eine Installation von Adware passieren.
Häufig verändert die Adware die Suchmaschine im Browser oder fügt Desktop-Symbole zu diversen Internetseiten hinzu. Adware ist meist eher lästig als ernsthaft schädlich, jedoch kann Adware auch in Form von Viren oder anderer Schadsoftware auftreten. Besonders bei kostenlosen Programmen sollte man aufmerksam sein, da sich diese vereinzelt durch Adware refinanzieren. Daher ist es ratsam, bei der Installation unbedingt darauf zu achten, dass keine zusätzlichen Komponenten (z.B. Toolbars etc.) installiert werden.
praxistipps.chip.de/adware-was-ist-das_35746

Bitcoin

Bei Bitcoins handelt es sich um eine virtuelle Währung, die seit dem Jahr 2009 existiert. Seitdem haben Bitcoins stetig an Bedeutung gewonnen und rasante Kursentwicklungen vollzogen. Während diese Währung anfangs nur bei wenigen für Aufsehen sorgte, beschäftigen sich heute sogar große Geldhäuser und Bankenaufsichten mit der Thematik. Für Anleger ist vor allem interessant, ob es sinnvoll ist, in Bitcoins zu investieren, ob sie eine sichere Anlage sein können und ob sich mit ihnen eine ansprechende Rendite erzielen lässt. Um Bitcoins besitzen und mit ihnen handeln zu können, braucht man zunächst lediglich einen Computer und die nötige Software – den sogenannten Bitcoin-Client. Hat man alle Voraussetzungen erfüllt, kann man auf Bitcoin-Marktplätzen Bitcoins erwerben und verkaufen. Ein Bitcoin existiert dann per Definition rein virtuell und der Besitz wird durch einen kryptografischen Schlüssel, einer Art Code oder Geheimtext, bewiesen.
www.gevestor.de/details/bitcoin-definition-und-erklarung-der-virtuellen-wahrung-687857.html

CEO E-Mail Scams

Beim Auftreten von CEO-E-Mail Scams erhält ein Mitarbeiter, z.B. aus der Finanzabteilung, vom vermeintlichen CEO den Auftrag per Mail, dass er eine Zahlung tätigen soll. Diese E-Mail kommt allerdings von einem externen Angreifer, der sich als Vorgesetzter ausgibt und dessen Konto irgendwo im Ausland liegt.
www.bison-its.ch/unternehmen/news/e-mail-scams

CEO Fraud bzw. Fake-President-Trick

Bei dieser Betrugsmasche geben sich die Täter als ein Organ des Unternehmens – meist ein Vorstandsmitglied bzw. eine vorgesetzte Person – aus und bitten per E-Mail oder Fax einen Mitarbeiter, der im Unternehmen für die Bankgeschäfte verantwortlich ist, eine dringende Überweisung auszuführen. Dem Mitarbeiter wird dabei vorgespiegelt, dass es sich um eine höchst geheime und vertrauliche Angelegenheit handelt.
Fast immer erfolgen die Geldtransfers auf ausländische Konten, vor allem in Asien und Osteuropa. Fliegt der Betrug dann auf, sind die Konten dort meist leergeräumt oder eine Rückholung wird aufgrund des ausländischen Rechtssystems erheblich erschwert.
Häufig werden gezielt Mitarbeiter in ausländischen Niederlassungen des Unternehmens angesprochen. Das erschwert den Mitarbeitern die persönliche Kontaktaufnahme mit den verantwortlichen Organen im Unternehmen, von denen die vermeintlichen Anweisungen kommen.
www.eulerhermes.de/veruntreuung/fake-president-fraud/Pages/default.aspx

Clickjacking

Clickjacking ist eine Technik, bei der ein Computerhacker die Darstellung einer Internetseite überlagert und dann deren Nutzer dazu veranlasst, scheinbar harmlose Mausklicks und/oder Tastatureingaben durchzuführen. Angreifer lassen die ahnungslosen Anwender – scheinbar – auf die überlagerten Objekte klicken. Tatsächlich wird jedoch der ursprüngliche Inhalt (Button/Link) der Internetseite ausgelöst. So geschieht es, dass der User – anstatt lediglich auf die ihm vorgegaukelten Links an einer Stelle zu klicken – eine vom Hacker definierte, beliebige Aktion auslöst.

de.wikipedia.org/wiki/Clickjacking

Cloud Computing

Der Begriff Cloud-Computing beschreibt sowohl das Nutzen als auch das Anbieten von verschiedensten IT-Dienstleistungen über ein Netzwerk. Dieser Prozess funktioniert dynamisch und an den Bedarf des Nutzers angepasst. Die Grundlage des Cloud-Computings ist das Internet beziehungsweise Intranet als Plattform. Über das Netz werden Verbindungen zu externen Servern hergestellt, wo verschiedene Anwendungen bereitgestellt werden. Unter Anderem ist hier die Möglichkeit zur Datenspeicherung oder Software-Anwendungen gemeint. So muss der Nutzer die verschiedenen IT-Services (Software, Plattformleistungen, Infrastrukturleistungen) nicht mehr selbst kaufen, sondern kann diese Leistungen über die Cloud in Anspruch nehmen, also mieten. Somit senkt Cloud-Computing die Kosten im IT-Bereich des Nutzers, da die kostenintensiven Investitionen wegfallen und nur noch variable Kosten während der Nutzung entstehen.

www.gruenderszene.de/lexikon/begriffe/cloud-computing

Computerwürmer

Ein Computerwurm ist ein Computerprogramm bzw. Skript mit der Eigenschaft, sich selbst zu vervielfältigen, nachdem es ausgeführt wurde. Ein Wurm ist eine Hacking-Technik und zählt zur Gruppe der Malware. Computerwürmer sind vollständige Programme, deren Lebensraum Rechnernetze sind. Sie verbreiten sich über Netzwerke oder über Wechselmedien wie USB-Sticks und können Kopien an andere Rechner verschicken. Im Gegensatz zu einem Virus wartet ein Wurm nicht passiv darauf, von einem Anwender auf einem neuen System verbreitet zu werden, sondern versucht, aktiv in neue Systeme einzudringen. Durch die Art, wie ein Wurm sich verbreitet, verbraucht er relativ hohe Netzwerkressourcen, was zur Überlastung bzw. sogar zum Ausfall von Servern führen kann.

wirtschaftslexikon.gabler.de/Definition/wurm.html

Computerviren

Ein Computervirus ist ein sich selbst verbreitendes Computerstörprogramm, das sich unkontrolliert in andere Programme einschleust, sich reproduziert, d.h. von sich selbst Kopien erzeugt, und diese dann in das bestehende Programm einpflanzt (infiziert) sobald es einmal ausgeführt wird. Dadurch gelangt der Virus auf andere Datenträger, wie Netzwerklaufwerke und Wechselmedien wie USB-Sticks.

wirtschaftslexikon.gabler.de/Definition/virus.html

Cyber-Angriffe

Ein Cyber-Angriff ist ein Angriff mit Mitteln der IT im Cyber-Raum, der sich gegen einen oder mehrere andere IT-Systeme richtet und zum Ziel hat, die Funktion der IT-Sicherheitssysteme zu brechen. Die Ziele der IT-Sicherheit, Vertraulichkeit, Integrität und Verfügbarkeit, können dabei als Teil oder Ganzes verletzt werden. Cyber-Angriffe, die sich gegen die Vertraulichkeit eines IT-Systems richten, werden als Cyber-Spionage bezeichnet und stellen somit Spionage auf digitalem Wege dar. Cyber-Angriffe gegen die Integrität und Verfügbarkeit eines IT-Systems werden als Cyber-Sabotage bezeichnet. (Vgl. Definition „Cyber" nach: Bundesministerium des Innern, „Cyber-Sicherheitsstrategie für Deutschland", Berlin, 2010)

www.bmi.gv.at/cms/cs03documentsbmi/1326.pdf

Cyber-Erpressung

Cyber-Erpressung ist ein Verbrechen, bei dem jemand über das Internet entweder angegriffen oder bedroht wird. Nur gegen Zahlung von Geld lässt sich dieser Angriff abwenden oder stoppen.

www.searchsecurity.de/definition/Cyber-Erpressung

Cyber-Mobbing

Der Begriff „Cyber-Mobbing" bezeichnet das absichtliche und über einen längeren Zeitraum anhaltende Beleidi-

gen, Bedrohen, Bloßstellen, Belästigen oder Ausgrenzen anderer über digitale Medien. Cyber-Mobbing findet vor allem im Internet (Soziale Netzwerke, Chats, Messenger, E-Mails, etc.) oder per Handy (SMS, lästige Anrufe, Messenger, Handyfotos und -videos, etc.) statt.
www.saferinternet.at/cyber-mobbing

Denial of Service

Denial of Service (DoS) sind Dienstverweigerungen, die im Internet zur Beeinträchtigung von Webservices führen und die, als DoS-Attacke ausgeführt, einen angegriffenen Server oder eine Website außer Betrieb setzen können.
DoS-Angriffe werden durch Überlastung von Servern ausgelöst, beispielsweise durch die Bombardierung eines Mail-Servers mit einer Flut an Mails, durch millionenfache Anfragen an einen Server oder durch Überflutung eines Netzwerks mit Datenpaketen. In allen Fällen können die Funktionen wegen Überlastung der Server oder Netze nicht mehr hinreichend ausgeführt werden. Die Server sind nicht mehr erreichbar, die Netze können zusammenbrechen.
www.itwissen.info/DoS-denial-of-service-DoS-Attacke.html

Firewall

Unter Firewall versteht man eine Hard- oder Software, die zwischen Rechner oder lokale Netzwerke und öffentliche Netze geschaltet wird, um den Zugriff auf Rechner von außen durch unbefugte Dritte zu verhindern und so interne Daten zu schützen. Auf einzelnen Rechnern installierte Firewalls, die mit dem Internet verbunden sind, werden Personal Firewall genannt.
wirtschaftslexikon.gabler.de/Definition/firewall.html

Hacker

Unter Hacker versteht man Personen, die sich über öffentliche Netze oder IP-Netze unberechtigten Zugang zu anderen Systemen verschaffen. Der unberechtigte Zugang erfolgt in der Regel unter Umgehung der Sicherheitssysteme. Hacker haben sicherheitsrelevante Kenntnisse und entwickeln Malware. Ihr Ziel ist die Überwindung von Sicherheitsmechanismen um Schwachstellen aufzudecken. Nach Überwindung der Sicherheitseinrichtungen haben sie Zugriff auf Netzwerke, virtuelle Maschinen und Datenbestände.
www.itwissen.info/Hacker-hacker.html

Identity Theft

Identity Theft bedeutet Identitätsdiebstahl, Identitätsbetrug. Es ist eine Methode bei der eine Person missbräuchlich die Identität einer anderen Person annimmt um unter falscher Identität auf Ressourcen und Datenbestände zugreifen zu können, auf die er ansonsten keinen Zugriff hätte.
Beim Identitätsdiebstahl benutzt der Dieb ohne Erlaubnis die Identität einer anderen natürlichen Person – dessen Name, Identitäts- oder Ausweisnummern, Kreditkarten- und Kontennummern – um damit im Internet Betrügereien oder andere kriminelle Handlungen zu begehen.
www.itwissen.info/Identitaetsdiebstahl-identity-theft.html

Malware

Siehe Schadsoftware
Malware (zusammengesetzt aus dem engl. malicious: bösartig und ware von Software) bezeichnet ein schädliches Programm (Schadsoftware). Dies sind Computerprogramme, die entwickelt wurden, um vom Benutzer unerwünschte bzw. schädigende Funktionen auszuführen (z.B. Viren, Computerwürmer, Trojaner, etc.).
wirtschaftslexikon.gabler.de/Definition/malware.html

Man-in-the-middle-Angriffe

Ein Man-in-the-Middle-Angriff (kurz: MITM-Angriff) bezeichnet einen Verschlüsselungsangriff in einem Rechnernetz. Dabei handelt es sich um einen dritten Host, der transparent als Gateway digitale Informationen zwischen zwei oder mehreren Kommunikationspartnern weiterleitet und gleichzeitig ausspäht. Der Absender und der Empfänger wissen dabei nicht, dass zwischen den beiden ein dritter Host existiert und dass sie eigentlich nicht direkt miteinander kommunizieren. Die häufigsten Angriffsziele sind gesicherte SSL-Verbindungen, wie z.B. beim Online-Banking. Bei einer Man-in-the-Middle Angriffsform hat der Angreifer vollständige Kontrolle auf die Informationen zwischen beiden oder mehreren Verbindungspartnern. Dadurch kann der unsichtbare Dritte die Informationen einlesen, beeinflussen und auch manipulieren. Der Angreifer spiegelt dabei die Identität des ersten und des zweiten Kommunikationspartners, damit er in den Kommunikationskanal eingreifen kann.

Die Informationen zwischen den beiden Hosts sind zwar verschlüsselt, dennoch werden diese durch den Angreifer entschlüsselt und weitergeleitet.
de.onpage.org/wiki/Man-in-the-middle

PC-Blockade
Eine PC-Blockade macht sich durch ein Hinweisfenster bemerkbar, das bei jedem regulären Systemstart erscheint und nicht geschlossen werden kann. Auch der Taskmanager wird blockiert. Unerfahrene PC-Benutzer wissen nicht, wie sie diese Blockade beenden können. Es scheint nur den Ausweg zu geben, das Lösegeld zu zahlen, indem beispielsweise eine Paysafecard oder Ukash-Karte gekauft wird. Der Betrag wird dem Erpresser gutgeschrieben, indem man die Gutscheinnummer des Bezahlsystems am befallenen PC eingibt, wodurch sie dem Täter elektronisch mitgeteilt wird. Als weitere anonyme Bezahlmethode wird die Kryptowährung Bitcoin eingesetzt.
de.wikipedia.org/wiki/Ransomware#Blockade_des_Systems

Pharming
Pharming ist eine Methode zum Betrug im Internet. Es ist der Versuch, durch manipulierte Websites in Betrugsabsicht an persönliche Informationen, z.B. Kreditkartendaten, zu kommen. Sie basiert auf einer Manipulation der DNS (Domain Name System)-Anfragen von Webbrowsern, um den Benutzer auf gefälschte Webseiten umzuleiten. Diese gefälschten Seiten befinden sich auf den Servern der Betrüger, die zu diesem Zweck große Server-Farmen betreiben; daher der Begriff. Pharming ist eine Weiterentwicklung des klassischen Phishings.
wirtschaftslexikon.gabler.de/Definition/pharming.html

Phishing
Phishing bedeutet, dass Daten von Internetnutzern beispielsweise über gefälschte Internetadressen, E-Mails oder SMS abgefangen werden. Die Absicht ist, persönliche Daten zu missbrauchen und Inhaber von Bankkonten zu schädigen. Der Begriff Phishing ist angelehnt an fishing (engl. für Angeln, Fischen) in Verbindung mit dem P aus Passwort, bildlich gesprochen das Angeln nach Passwörtern mit Ködern. Begriffstypisch ist dabei die Nachahmung des Designs einer vertrauenswürdigen Website.
wirtschaftslexikon.gabler.de/Definition/phishing.html

Ransomware/Kryptho-Trojaner
Ransomware (Ransom = Lösegeld oder Freilassung) sind Lösegeldprogramme, die als Malware im Anhang von E-Mails versandt werden und Programme, Bootsektoren oder Dateien befallen und den Rechner außer Betrieb setzen. Ransomware wird auch als Krypto-Virus, Krypto-Trojaner oder Krypto-Wurm bezeichnet.
www.itwissen.info/Ransomware-ransomware.html

Schadsoftware
Schadsoftware, auch Malware (zusammengesetzt aus dem engl. malicious: bösartig und ware von Software), bezeichnet ein schädliches Programm. Dies sind Computerprogramme, die entwickelt wurden, um vom Benutzer unerwünschte bzw. schädigende Funktionen auszuführen (z.B. Viren, Computerwürmer, Trojaner, etc.).
wirtschaftslexikon.gabler.de/Definition/malware.html

Spear-Phishing
Bei Spear-Phishing handelt es sich um spezielle Betrugsversuche per E-Mail. Sie richten sich meist gegen konkrete Organisationen und zielen darauf ab, nicht autorisierten Zugriff auf vertrauliche Daten zu erhalten. Die Hintermänner bei Spear-Phishing sind nicht die üblichen Hacker, die willkürlich Daten abgreifen. Vielmehr geht es hier häufig gezielt um Finanzbetrug, Abschöpfen von Geschäftsgeheimnissen oder sogar militärische Informationen. Die für eine Spear-Phishing-Kampagne verwendeten E-Mails scheinen ebenso wie bei normalen Phishing-Kampagnen von einer vertrauenswürdigen Quelle zu stammen. Als Absender wird in der Regel ein großes und bekanntes Unternehmen oder eine Internet-Plattform mit hoher Mitgliederzahl angegeben. Für Spear-Phishing tarnt sich der Absender der E-Mail allerdings eher als Mitarbeiter im Unternehmen des Empfängers und gibt sich häufig als ein Vorgesetzter aus.
www.searchsecurity.de/definition/Spear-Phishing

Spyware
Als Spyware wird jede Technologie bezeichnet, die dabei hilft, Informationen über eine Person oder Organisation ohne deren Wissen zu sammeln. Im Zusammenhang

mit dem Internet handelt es sich bei Spyware (manchmal auch als Spybot oder Tracking Software bezeichnet) um eine Software, die heimlich auf dem Computer oder mobilen Gerät eines Internetnutzers installiert wird, um Informationen über diesen Anwender zu sammeln und an Werbetreibende oder andere daran interessierte Personen weiterzuleiten. Spyware kann mit Hilfe eines Softwarevirus oder bei der Installation einer neuen Anwendung auf den Computer gelangen.
www.searchsecurity.de/definition/Spyware

Trojaner

Als Trojanisches Pferd (engl. Trojan Horse, kurz Trojaner), bezeichnet man ein Computerprogramm, das gezielt auf fremde Computer eingeschleust wird oder zufällig dorthin gelangt und nicht genannte Funktionen ausführt. Es ist als nützliches Programm getarnt, indem es beispielsweise den Dateinamen einer nützlichen Datei aufweist oder neben der versteckten Funktion tatsächlich eine nützliche Funktionalität aufweist.
wirtschaftslexikon.gabler.de/Definition/trojaner.html

Zeit- oder Logik-Bomben

Eine „Bombe" führt eine bestimmte, schädliche Handlung aus, wobei die Ausführung abhängig gemacht wird von der Erfüllung einer bestimmten Bedingung (des „Triggers").
Demnach sind Bomben als „getriggerte Trojaner" als Spezialfall des Trojanischen Pferdes anzusehen.
Nach Art des Triggers kann man die Bomben einteilen in folgende Untertypen:
Ist der Trigger eine logische (boolesche) Bedingung, spricht man von einer Logik-Bombe (oder auch „logische Bombe").
Bei Zeitbomben stellt eine zeitliche Bedingung die Trigger-Variable dar. Signalbomben warten auf ein bestimmtes Signal, bevor sie ihren Schadensteil ausführen.
Oft sind Bomben Teil eines größeren Programmes.
agn-www.informatik.uni-hamburg.de/papers/publications/hct/VTC.pdf

Whaling

Der Ausdruck „Whaling" ist eine Anspielung auf die phonetische Ähnlichkeit mit (engl.) Phishing und Fishing (fischen). Es ist eine Form der Internetkriminalität und wird Whaling genannt, weil man damit „große Fische" (engl. whale: Wal), i.d.R. Führungskräfte angeln, d.h. betrügen will. Dadurch wollen die Betrüger ihre Opfer dazu verleiten, einen Link zu nutzen, der angeblich zu mehr Information, wie z.B. zur vollständigen Version eines Schreibens führt. In Wahrheit verbirgt sich dahinter jedoch ein Malware-Download. Beim Whaling kommen angepasste Betrugs-E-Mails zum Einsatz.
wirtschaftslexikon.gabler.de/Definition/whaling.html

Gedruckt auf CO_2-ausgeglichenem Papier

Die Inhalte dieser Unterlage wurden mit größtmöglicher Sorgfalt zusammengestellt, dennoch übernimmt die Allianz keine Haftung für die Richtigkeit, Vollständigkeit und Aktualität der enthaltenen Informationen.
Die Allianz ist bemüht, die in dieser Unterlage enthaltenen Informationen, insbesondere bei Vorliegen eines Bedarfs, zu aktualisieren, jedoch übernimmt sie hierfür keine Verpflichtung.

Aus dieser Unterlage können keine Rechtsansprüche – gleichgültig welcher Art – abgeleitet werden.

Regelungen bezüglich der Selbstbehalte finden sich in den Allgemeinen, Ergänzenden Allgemeinen und Besonderen Versicherungsbedingungen.
Der angeführte Leistungsumfang stellt einen Auszug aus den Allgemeinen, Ergänzenden Allgemeinen und Besonderen Versicherungsbedingungen dar. Diese werden dadurch nicht ersetzt. Vollständige Informationen entnehmen Sie bitte dem Antrag, der Versicherungsurkunde und den jeweiligen Versicherungsbedingungen.

Bei allen personenbezogenen Bezeichnungen (z.B. Versicherungsnehmer, Vertragspartner, Sachverständiger, etc.) gilt die gewählte Bezeichnung für beide Geschlechter.

Änderungen, Irrtümer und Druckfehler vorbehalten.
Stand der Informationen Juni 2017

Allianz Elementar Versicherungs-Aktiengesellschaft,
Sitz: 1130 Wien, Hietzinger Kai 101–105
Telefon: 05 9009-0, Telefax: 05 9009-70000
Eingetragen im Firmenbuch des Handelsgerichts Wien
unter FN 34004g, UID: ATU 1536 4406, DVR: 0003565
Internet: http://www.allianz.at

Aufsichtsbehörde:
Finanzmarktaufsicht, 1090 Wien, Otto-Wagner-Platz 5, www.fma.gv.at

50452 (08.17)_wes