Vertragsbestandteil C 03.2

Erläuterungen zu Ihrer Cyberversicherung

Juni 2022

ALTE LEIPZIGER
ZUKUNFT BEGINNT HEUTE.

Cyberschutz für Gewerbekunden

Die folgenden Ausführungen dienen der Veranschaulichung der wichtigsten Aspekte Ihrer Cyberversicherung bei der ALTE LEIPZIGER Versicherung AG. Der rechtsverbindliche Umfang des Versicherungsschutzes geht ausschließlich aus den diesem Vertrag zugrunde liegenden Versicherungsbedingungen hervor.

Was ist versichert?

Versichert sind Vermögensschäden (keine Personen- oder Sachschäden), die durch eine Verletzung der Informationssicherheit verursacht worden sind.

Eine Informationssicherheitsverletzung liegt in folgenden Fällen vor:

- Ihre elektronischen Daten wurden verändert, sind für Sie nicht mehr verfügbar oder werden Unberechtigten zugänglich.
- Ihre IT-Systeme funktionieren nicht mehr korrekt oder sind für Sie nicht mehr zugänglich.

Eine Informationssicherheitsverletzung muss durch folgende Ereignisse ausgelöst werden:

- Angriff oder unberechtigter Zugriff auf Ihre elektronischen Daten
- Angriff auf oder Eingriff in Ihre IT-Systeme
- Schadprogramme wirken auf Ihre elektronischen Daten oder IT-Systeme

Damit besteht Versicherungsschutz u. a. für folgende Fälle:

- Hacker-Angriff auf Ihre elektronischen Daten oder IT-Systeme (z. B. Löschung, Beschädigung, Kopie, Blockierung)
- DoS-/DDoS-Angriff stört oder unterbricht Ihre IT-Systeme
- Computervirus/-wurm, Trojaner oder andere Schadsoftware wirken auf Ihre elektronischen Daten oder IT-Systeme
- Betrügerisches Erlangen Ihrer Zugangsdaten/Passwörter über gefälschte E-Mails/Websites (Phishing) oder DNS-Abfragen (Pharming), Manipulation Ihrer Website oder missbräuchliche Nutzung Ihrer Identität
- Rechtswidriges Verschlüsseln Ihrer Daten und Erpressung einer Lösegeldzahlung für die Entschlüsselung
- Vorsätzliche Schädigung durch Ihren Mitarbeiter
- Unsachgemäße Bedienung Ihrer IT-Systeme

Versicherungsschutz besteht für Versicherungsfälle weltweit. Dies gilt jedoch nur, soweit die Ansprüche in EWR-Staaten und nach deren Recht geltend gemacht werden. Für Betriebsstätten und IT-Systeme (z. B. Server, Produktions- oder Vertriebsniederlassungen, Läger), die Sie selbst betreiben, besteht Versicherungsschutz ausschließlich innerhalb der Bundesrepublik Deutschland.

Nähere Informationen finden Sie in den allgemeinen Regelungen zum Versicherungsschutz, welche unter A 1 der Allgemeinen Bedingungen für die Cyberversicherung (ACB) aufgeführt sind.

Soforthilfe im Notfall

Bei Bestehen einer konkreten Notfallsituation übernimmt die ALTE LEIPZIGER die Kosten eines Dienstleisters für eine 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).

Eine Notfallsituation liegt vor, wenn aus Ihrer Sicht der tatsächliche oder der künftige Eintritt eines versicherten Cyberschadens zu vermuten ist. Konkrete Anhaltspunkte dafür können sein:

- Meldung einer Infektion der IT-Systeme durch die Antivirensoftware oder Firewall
- Auffälligkeiten in den Logdateien der Antivirensoftware oder Firewall

Bei einem Cyberangriff können die ersten Stunden entscheidend sein. Der Dienstleister kann deshalb seinen Verpflichtungen nur dann in vollem Umfang nachkommen, wenn die Notfallsituation schnellstmöglich angezeigt wird. Melden Sie also den eingetretenen oder bevorstehenden Schaden unverzüglich unter der folgenden Rufnummer:

Telefonnummer für die Cyber-Soforthilfe:

06171 66-2206

Dieser Notrufservice steht Ihnen rund um die Uhr, d. h. 24 Stunden am Tag und 7 Tage die Woche, zur Verfügung. Hinsichtlich der Kosten für die Soforthilfe fällt weder eine Selbstbeteiligung an noch werden diese Kosten auf die Deckungssumme angerechnet. Dies gilt jedoch nur, sofern Sie die Notfallsituation über unsere Telefonnummer für die Cyber-Soforthilfe melden und somit der von der ALTE LEIPZIGER beauftragte Dienstleister die telefonische Soforthilfe durchführt.

Präventionsleistungen

Die ALTE LEIPZIGER stellt Ihnen folgende kostenlose Präventionsleistungen über eine Online-Plattform zur Verfügung:

- Digitale Schulungen zu Themen der IT-/Datensicherheit
- Phishing-Simulationen in Form fingierter E-Mails

Diese Präventionsmaßnahmen können von Ihnen und den mitversicherten Personen und Unternehmen jährlich durchgeführt werden.

Erbringen Sie im Schadenfall den Nachweis, dass mindestens 75 % der mitversicherten Personen sowohl Ihres Unternehmens als auch der mitversicherten Unternehmen jährlich über die von der ALTE LEIPZIGER zur Verfügung gestellte Online-Plattform

- die digitalen Schulungen zu Themen der IT-/Datensicherheit erfolgreich absolviert haben und
- der Phishing-Simulationen unterzogen wurden,

so reduziert sich für diesen Schadenfall die im Versicherungsschein festgelegte monetäre Selbstbeteiligung um 50 %. (Diese Regelung gilt nicht für die zeitliche Selbstbeteiligung im Rahmen des Zusatzmoduls Betriebsunterbrechung).

Der Nachweis über die durchgeführten Präventionsmaßnahmen muss für das aktuelle Versicherungsjahr, in dem der Schadenfall eingetreten ist, erbracht werden. Sofern Sie im aktuellen Versicherungsjahr die Präventionsmaßnahmen noch nicht im erforderlichen Umfang durchgeführt haben, so genügt der Nachweis für das vorherige Versicherungsjahr.

Die Registrierung auf der online-Plattform erfolgt unter folgendem Link:

https://alte-leipziger.cyberdirekt.de

Hier erhalten Sie auch alle relevanten Informationen zur Nutzung der Präventionsleistungen.

Leistungen bei Eigenschäden

Unter A 2 der Allgemeinen Bedingungen für die Cyberversicherung (ACB) sind die Leistungen des Eigenschaden-Bausteins aufgeführt, welche nachfolgend in einer Kurzübersicht dargestellt werden.

Modul Eigenschaden

Dieses Modul stellt die Grunddeckung der Cyberversicherung dar und ist daher immer mitversichert. Es beinhaltet die Erstattung der Kosten bzw. Aufwendungen für folgende Positionen:

- Ermittlung der Ursache und Feststellung des versicherten Schadens (IT-Forensik). Stellt sich heraus, dass kein versichertes Schadenereignis eingetreten ist, werden die bis dahin aufgewendeten Ermittlungskosten erstattet.
- Wiederherstellung der betroffenen Daten und Entfernung der Schadsoftware
- Honorare von beauftragten Sicherheitsberatern einschließlich der Kosten für angemessene Sicherheitsverbesserungen nach einem Angriff
- Krisenkommunikation und PR-Maßnahmen zur Wiederherstellung der öffentlichen Reputation
- Abwendung der Bedrohungslage bei einer Cyberbedrohung/-erpressung sowie Krisenberatung und -management
- Überwachung und Prüfung von EC-/Kreditkartendaten (Monitoring Service)
- Abhandenkommen von Geldern inkl. Guthaben bei Online-Bezahlsystemen sowie entstandene Telefonmehrkosten/-gebühren (inkl. Voiceover-IP) und erhöhte Versorgungsrechnungen
- Verluste im elektronischen Zahlungsverkehr durch falsch ausgeführte, umgeleitete oder manipulierte Überweisungen
- Maßnahmen zur Vermeidung eines unmittelbar bevorstehenden Schadens
- Schadenminderung
- Sachschäden an IT-Systemen

Zusatzmodul Betriebsunterbrechung

Dieses Zusatzmodul kann optional vereinbart werden und beinhaltet die Erstattung des entgangenen Betriebsgewinns und der fortlaufenden Kosten, die Sie im Zeitraum einer Betriebsunterbrechung, die durch einen versicherten Cyberschaden in Ihrem Betrieb oder bei einem entgeltlich beanspruchten Dienstleister (z. B. Cloud-Anbieter) ausgelöst wird, nicht erwirtschaften können. Mitversichert sind auch Mehrkosten, die Sie für die Fortführung Ihres Betriebes aufwenden müssen (z. B. Nutzung fremder IT-Systeme).

Zusatzmodul CEO-Fraud

Dieses Zusatzmodul kann optional vereinbart werden und beinhaltet die Erstattung missbräuchlich entwendeter Geldbeträge, die durch eine Vertrauensperson ausgezahlt wurden, weil ein unbefugter Dritter sich als Mitglied der Geschäftsführung ausgegeben hat und die Vertrauensperson zu dieser Zahlung angewiesen hat.

Leistungen bei Drittschäden

Unter A 3 der Allgemeinen Bedingungen für die Cyberversicherung (ACB) sind die Leistungen des Drittschaden-Bausteins aufgeführt, welche nachfolgend in einer Kurzübersicht dargestellt werden.

Modul Drittschaden

Dieses Modul kann optional vereinbart werden und bietet Versicherungsschutz für den Fall, dass Sie wegen einer Informationssicherheitsverletzung von einem Dritten auf Schadensersatz in Anspruch genommen werden

- aufgrund gesetzlicher Haftpflichtbestimmungen privatrechtlichen Inhalts;
- wegen Persönlichkeitsrechts-, Namensrechts-, Urheberrechts- oder Markenrechtsverletzungen (und daraus resultierende Verstöße gegen das Wettbewerbsrecht) durch von Ihnen veröffentlichte elektronische Medieninhalte.

Im Rahmen des Moduls Drittschaden zusätzlich einschließbar:

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

Zusatzmodul Datenschutz

Dieses Zusatzmodul kann optional vereinbart werden und beinhaltet Versicherungsschutz für Schadensersatzansprüche, die gegen Sie wegen einer Verletzung von datenschutzrechtlichen Vorschriften aufgrund einer Informationssicherheitsverletzung geltend gemacht werden. Mitversichert sind auch DSGVO-Bußgelder (sofern versicherbar) sowie die Kosten für die Rechtsberatung zu Informationspflichten, für die Benachrichtigung betroffener Dateninhaber und für die Beauftragung eines externen Call-Centers oder die Einrichtung einer speziellen Website zur Beantwortung von Rückfragen.

Zusatzmodul E-Payment

Dieses Zusatzmodul kann optional vereinbart werden und beinhaltet Versicherungsschutz für Forderungen zur Zahlung von Vertragsstrafen, die ein E-Payment Service Provider wegen einer Verletzung eines Payment Card Industry (PCI) Datensicherheitsstandards gegen Sie geltend macht.

Festlegung der Deckungssummen und Selbstbeteiligungen

Die Deckungssummen und Selbstbeteiligungen können für den ganzen Vertrag (pauschal für die komplette Cyberpolice), je Baustein (d.h. für den Eigenschaden-Baustein und - sofern gewählt - für den Drittschaden-Baustein) oder für jedes einzelne Modul festgelegt werden.

Die einzelnen Module können unabhängig von der Art der Summenfestlegung ausgewählt werden. Für das Zusatzmodul Betriebsunterbrechung muss die zeitliche Selbstbeteiligung immer festgelegt werden.

Obliegenheiten zur Gewährleistung der IT-Sicherheit

Bei Vertragsabschluss bestätigen Sie, 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. Viren)
- Regelmäßige Sicherheitsupdates
- Mindestens wöchentliche Datensicherung (Sicherungsdatenträger physisch getrennt von den Originaldaten aufbewahrt)
- Schriftlich fixiertes IT-Notfall- und Wiederanlaufkonzept (gilt ab 5 Mio. EUR Jahresumsatz)
- Einhaltung aller gesetzlichen, behördlichen sowie vertraglich vereinbarten Sicherheitsvorschriften

Bitte beachten Sie, dass es sich hierbei um Kurzbeschreibungen handelt. Den rechtsverbindlichen Wortlaut sowie nähere Erläuterungen und Empfehlungen hierzu können Sie dem diesem Vertrag zugrunde liegenden Dokument „Obliegenheiten vor Eintritt des Versicherungsfalls zur Gewährleistung der IT-Sicherheit“ entnehmen.

Glossar

Nachfolgend werden einige wichtige Fachbegriffe aus dem Cyberumfeld erläutert. Diese werden größtenteils auch in den Vertragsbestandteilen Ihrer Cyberversicherung genannt und können hier ergänzend nachgelesen werden.

Administrator

Der Administrator ist ein Verwalter eines Systems (z. B. Netzwerk, Computer). Er ist für die Wartung und Sicherstellung des fortlaufenden Systembetriebs sowie die Systemsicherheit zuständig. Dafür besitzt er die erforderlichen Zugriffsrechte und kann die Rechte anderer Systemnutzer einsehen und ggf. auch einschränken.

Back-up (Datensicherung)

Bei einem Back-up werden Daten auf ein separates Medium (z. B. externe Festplatte) kopiert, um im Falle eines Datenverlustes die Originaldaten wiederherstellen zu können.

Botnet (Botnetz)

Bei einem Botnetz handelt es sich um ein zentral von Kriminellen errichtetes und steuerbares Netzwerk infizierter Computer oder internetfähiger Geräte (z. B. Überwachungskameras). Diese mit Schadsoftware infizierten Computer/Geräte werden Bots (von Roboter) genannt, da sie ohne das Einverständnis ihres rechtmäßigen Nutzers von außen gesteuert

werden können. Botnetze werden z. B. für DDoS-Attacken eingesetzt und von ihren Betreibern gegen Entgelt an andere Kriminelle vermietet.

Bring Your Own Device (BYOD)

Bring Your Own Device beschreibt die gewollte Einbindung privater mobiler Endgeräte wie Notebooks, Tablets oder Mobiltelefone in Unternehmensnetzwerke zur dienstlichen Nutzung.

Cloud-Computing

Cloud-Computing umfasst ein Netzwerk aus IT-Strukturen und IT-Leistungen (z. B. Rechenleistung, Software oder Speicherplätze), die von entsprechenden Dienstleistern über das Internet bereitgestellt werden. Im Cloud-Computing ist es nicht mehr notwendig, Daten lokal auf dem Rechner zu speichern, da sie online in einer Cloud bearbeitet und gespeichert werden können.

Denial-of-Service-Attacke (DoS-Attacke)

Denial of Service (DoS) bedeutet "Verweigerung des Dienstes". Eine DoS-Attacke ist ein zielgerichteter Angriff auf ein mit dem Internet verbundenes System (z. B. Server oder Website) mit der Absicht, dieses durch eine Vielzahl von Anfragen zu überlasten und somit zu stören oder zu unterbrechen.

Distributed-Denial-of-Service-Attacke (DDoS-Attacke)

Eine DDoS-Attacke ist eine DoS-Attacke, die mittels einer Vielzahl von Computern oder internetfähiger Geräte erfolgt (siehe „Botnet“) und von diesen zum gleichen Zeitpunkt ausgelöst wird. Dadurch ist sie nur schwer zu orten und noch schwieriger zu unterbinden.

DSGVO

Die Datenschutz-Grundverordnung (DSGVO) der EU regelt die Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen. Sie soll sicherstellen, dass personenbezogene Daten innerhalb der EU geschützt sind, gleichzeitig aber den freien Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleisten.

E-Payment Service Provider

Der elektronische Zahlungsverkehr über das Internet wird als E-Payment bezeichnet. Ein E-Payment Service Provider erbringt entgeltlich Zahlungsdienstleistungen wie z. B. die Anbindung von Online-Bezahlmethoden bei Online-Shops und die Zahlungsabwicklung.

Firewall

Eine Firewall ist ein zwischen Computern oder Netzwerken installiertes Softwarepaket (manchmal auch im Zusammenhang mit eigener Hardware), das einen kontrollierten und reglementierten Datenaustausch sicherstellt und so unbefugte Zugriffe von oder nach außen verhindert.

Hosting

Als Hosting wird der Betrieb von Softwareapplikations- oder Internetdiensten bezeichnet. Ein Webhosting-Anbieter (Hosting-Provider) bietet und betreibt Hosting-Dienste für Angebote seiner Kunden im Internet, wie z. B. eine E-Commerce-Shopping-Website.

Industrial Control System (ICS)

Industrial Control System ist ein Oberbegriff für industrielle Steuerungssysteme (Fabrikautomation und Prozesssteuerung) mit einer Infrastruktur aus Hardware, Software und Vernetzungskomponenten.

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.

Kompromittieren

Das unberechtigte Eindringen in ein Computersystem und das dortige Ausspähen oder Manipulieren gespeicherter Daten wird als Kompromittieren bezeichnet.

Logdatei

Bei einer Logdatei (auch Logfile genannt) handelt es sich um eine Protokolldatei, in der IT-Systeme Ereignisse in Computersystemen oder Netzwerken eintragen und protokollieren. Die Datei soll helfen, Vorgänge nachvollziehbar zu machen, um so beispielsweise für die Problemanalyse oder die Rekonstruktion von verloren gegangenen Daten herangezogenen werden zu können.

Netzwerk

Bei einem Netzwerk spricht man (im Bereich der Informationstechnik) von Computern bzw. netzwerkfähigen Geräten, die zu einem System zum Zweck der Datenkommunikation zusammengeschlossen sind. Man unterscheidet lokale Netzwerke (LAN/WLAN) oder überregionale Netzwerke (WAN).

Payment Card Industry Data Security Standard (PCI-DSS)

Der Datensicherheitsstandard der Payment Card Industry (Zusammenschluss der großen Kreditkartenunternehmen) ist ein Regelwerk für die Abwicklung von Kreditkartentransaktionen und hat das Ziel, Kreditkartendaten vor Diebstahl und Missbrauch zu schützen. Alle Unternehmen, die Kreditkartenzahlungen akzeptieren und die entsprechenden Daten verarbeiten, müssen diese Regelungen und Sicherheitsstandards erfüllen.

Pharming

Als Pharming wird eine betrügerische Methode beschrieben, mit der Nutzer bei Eingabe einer Webadresse automatisch auf eine gefälschte Website weitergeleitet werden, um vertrauliche Nutzerdaten ausspionieren zu können. Die Nutzer merken oftmals nicht, dass sie sich auf einer gefälschten Seite befinden, und geben arglos ihre persönlichen Daten ein. Kreditkartenbetrug und die Manipulation von Online-Banking-Zugängen sind hier häufig das Ziel. Die Methode basiert auf der Idee des Phishings.

Phishing

Phishing beschreibt den Versuch, durch falsche Informationen Nutzer dazu zu bringen, persönliche Zugangsdaten wie Benutzernamen und Passwörter im Web preiszugeben. Getarnt werden die Angriffe über gefälschte E-Mail-Links oder Webadressen, um einen seriösen Anschein zu erwecken. Besonders lukrativ und beliebt ist bei Betrügern der Diebstahl von Kontodaten.

Ransomware

Bei Ransomware handelt es sich um eine Schadsoftware, die oft über Phishing-Mails auf das Computersystem der Nutzer gelangt und das Ziel hat, den Zugriff darauf zu blockieren oder die dort gespeicherten Daten zu verschlüsseln, um dann von den Nutzern Löse-/Erpressungsgelder für die Entschlüsselung oder Freigabe zu fordern.

Schadsoftware (Malware)

Als Schadsoftware, Schadenprogramme oder Malware werden Computerprogramme bezeichnet, die schädigende und vom Systembesitzer unerwünschte Wirkung entfalten, wenn sie auf dessen Systeme gelangen. Beispiele: Viren, Würmer, Trojaner, Ransomware.

Server

Ein Server ist ein Computerprogramm oder Computer, der über ein Netzwerk anderen Computern oder Programmen ("Clients") Dienste, Daten oder andere Ressourcen, wie z. B. Speicherkapazität, bereitstellt.

Sicherheitspatch

Sicherheitspatches sind Nachbesserungen, die identifizierte Sicherheitslücken schließen (siehe auch „Update“). Sie werden von Softwareherstellern in regelmäßigen Abständen an die Nutzer verteilt und sollten von diesen implementiert werden.

Social Engineering

Beim Social Engineering nutzen Angreifer die Hilfsbereitschaft oder das Vertrauen ihrer Opfer aus, um sie durch geschickte Manipulation beispielsweise dazu zu verleiten, vertrauliche Informationen preiszugeben, Sicherheitsfunktionen auszuhebeln oder Schadsoftware zu installieren. Beispielsweise gibt sich der Angreifer als Systemadministrator aus und ruft den Mitarbeiter an, da er angeblich zur Behebung eines Sicherheitsproblems oder Systemfehlers das Passwort des Benutzers benötigt.

Software as a Service (SaaS)

Bei Software as a Service (SaaS) wird die Software und die IT-Infrastruktur bei einem externen Dienstleister betrieben und vom Anwender als entgeltliche Dienstleistung über das Internet als Cloud-Anwendung genutzt.

Trojaner

Ein Trojaner (Trojanisches Pferd) ist eine Software, die sich - offiziell als nützliches Anwendungsprogramm getarnt - auf dem Computersystem einschleicht, und im Hintergrund unbemerkte Funktionen ausführt, um den Anwender und sein System zu schädigen.

Update

Als Update wird die Aktualisierung von Datenbanken oder Software-Anwendungen bezeichnet. Die regelmäßig angebotenen Updates dienen meist dazu, Sicherheitslücken zu schließen oder die Software um neue Funktionalitäten und Verbesserungen zu erweitern. Spezielle Sicherheitsupdates gibt es vor allem für Betriebssysteme, Firewalls oder Antivirenprogramme.

Verschlüsselung

Bei der Verschlüsselung von Daten werden diese in ein unleserliches Format umgewandelt, um sie vor unbefugtem Zugriff zu schützen. Erst nach der Entschlüsselung mit einem geheimen Schlüssel (z. B. Passwort) können die Daten wieder gelesen werden. Die Verschlüsselung ist daher eine der wichtigsten Voraussetzungen, um die Datensicherheit gewährleisten zu können. Dies gilt besonders für den Versand datenschutzrelevanter Daten (z. B. beim Online-Banking). Bei der zertifikatsbasierten Verschlüsselung kommen innerhalb einer Sicherheitsinfrastruktur, der sogenannten Public-Key-Infrastruktur (PKI), digitale Zertifikate zur Anwendung, um einen sicheren Austausch von Daten zwischen Kommunikationspartnern im Internet zu gewährleisten. Das digitale Zertifikat ist ein elektronischer Echtheitsnachweis, der von einer Zertifizierungsstelle ausgestellt wird und die vergleichbare Funktion eines Personalausweises besitzt.

Virenscanner

Ein Virenscanner, auch Antiviren- oder Virenschutz-Programm genannt, ist ein Programm, das Schadsoftware (Viren, Würmer, Trojaner) auf Systemen identifizieren und gegebenenfalls auch eliminieren soll. Wichtig ist dabei, den Virenscanner durch regelmäßige Updates möglichst aktuell zu halten, sodass ihm die "Steckbriefe" zur Identifikation der Schadsoftware vorliegen.

Virtual Private Network (VPN)

Ein Virtual Private Network bezeichnet ein privates, virtuelles Netzwerk, das bereits in einem bestehenden Kommunikationsnetzwerk integriert ist und die Teilnehmer eines Netzes an ein anderes bindet. So können z. B. Mitarbeiter über ein VPN als Firmennetzwerk nicht nur am Arbeitsplatz im Unternehmen, sondern auch von Zuhause aus auf dieses zugreifen.

Virus

Ein Computervirus ist ein Schadprogramm, welches sich im Computersystem ausbreitet. Es benötigt eine Nutzeraktion für seine Verbreitung. So gelangt der Virencode z. B. durch das Öffnen einer infizierten Datei auf weitere Systeme und infiziert diese.

WLAN

Ein WLAN (Wireless Local Area Network) bezeichnet ein drahtloses lokales Netzwerk, das einen kabellosen Internetzugriff ermöglicht.

WPA

Bei WPA (Wi-Fi Protected Access) handelt es sich um eine Technik zur Datenverschlüsselung im Bereich von WLAN. Die Nachfolger WPA2 und WPA3 wenden einen anderen Verschlüsselungsalgorithmus an.

Wurm

Ein Computerwurm ist ein Schadprogramm, das sich selbstständig in Netzen verbreitet, ohne dabei Dateien zu infizieren.

Zwei-Faktor Authentisierung

Zwei-Faktor Authentisierung bezeichnet den Identitätsnachweis eines Nutzers mittels der Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten (z. B. Bankkarte und PIN).