VHV CYBER-LEXIKON

VHV VERSICHERUNGEN

WIE GUT SPRECHEN SIE CYBERANISCH?

Beim Schutz Ihrer Netzwerke und Daten werden Sie früher oder später mit hoch spezialisierten IT-Experten sprechen.

Und die haben ihre ganz eigene Art, sich auszudrücken: Deren Sprache besteht aus technischen Abkürzungen („CSRF“), englischen Fachbegriffen („Zero-Day-Exploit“) und dem Insider-Jargon der Hackerszene. Letztere ist im Erfinden neuer Wörter äußerst kreativ und bereicherte die IT-Sprache u. a. um „Phishing“, „Nicknapping“ oder „Fuzzing“.

Auch wenn sich dieses „Cyberanisch“ etwas sonderbar anhört: Es ermöglicht Ihnen, sich über Computerschäden hochpräzise zu verständigen. Darum hat die VHV die wichtigsten Begriffe hier für Sie gesammelt und leicht verständlich erklärt.

Dieses Taschenwörterbuch hilft Ihnen, die Welt der Cyberrisiken zu verstehen und gibt Ihnen mehr Sicherheit im Gespräch mit Fachleuten.

Gleichzeitig hoffen wir, dass Sie keinen der Fachausdrücke je benutzen müssen und Ihr IT-System immer störungsfrei läuft!

DAS KLEINE ABC DER CYBERWELT

A.

ADBLOCKER
Ein „Adblocker“ ist eine Anwendung, die verhindern soll, dass Werbung auf Websites angezeigt wird. Sie erkennen einen Großteil der im Internet geschalteten Werbeanzeigen und blenden diese aus. Einige Adblocker können jedoch auch Spyware beinhalten.

ADVANCED PERSISTENT THREAT (APT)
„Advanced Persistent Threats“ (APT) sind zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer dauerhaften Zugriff zu einem Netz verschafft und diesen in der Folge auf weitere Systeme ausweitet. Hierzu sind hohe Ressourceneinsätze und erhebliche technische Fähigkeiten aufseiten der Angreifer nötig.

B.

BOTNETZE
Als „Botnetz“ wird ein Verbund von Rechnern (Systemen) bezeichnet, die von einem fernsteuerbaren Schadprogramm (Bot) befallen sind. Die betroffenen Systeme werden vom Botnetz-Betreiber mittels eines Command-and-Control-Servers (C&C-Server) kontrolliert und gesteuert.

C.

CACHE POISONING

Unter „Cache Poisoning“ versteht man das Einschleusen von manipulierten Daten in einen Zwischenspeicher „Cache“, der dann von anderen Anwendungen oder Diensten genutzt wird. Ein Angreifer kann so z. B. allgemein die Routen von Datenpaketen ändern oder gezielt Anfragen für Webseiten einer Bank auf eine gefälschte Seite umleiten.

CSRF

„Cross-Site-Request-Forgery“ ist eine weitere Angriffsform, die sich gegen Benutzer von Webanwendungen richtet. Mit dieser Vorgehensweise lassen sich Funktionen einer Webanwendung von einem Angreifer im Namen des Opfers nutzen. Ein Beispiel ist die Versendung einer gefälschten Statusnachricht in einem sozialen Netzwerk: Ein Angreifer formuliert die Nachricht und schiebt sie dem Opfer beim Abruf einer Webseite unter. Wenn der Angriff gelingt und das Opfer während des Angriffs parallel im betreffenden sozialen Netzwerk angemeldet ist, wird die Nachricht des Angreifers im Namen des Opfers veröffentlicht.

CHOSEN-PLAINTEXT-ATTACKE

Kryptografischer Angriff, in dem der Angreifer Zugriff auf Chiffrate zu von ihm gewählten Klartexten erhalten kann.

CYBERRAUM

Der Cyberraum ist der virtuelle Raum aller weltweit auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme. Dem Cyberraum liegt als öffentlich zugängliches Verbindungsnetz das Internet zugrunde, welches durch beliebige andere Datennetze erweitert werden kann.

D.

DATENSICHERUNG

Bei einer Datensicherung werden zum Schutz vor Datenverlust Sicherungskopien von vorhandenen Datenbeständen erstellt. Datensicherung umfasst alle technischen und organisatorischen Maßnahmen zur Sicherstellung der Verfügbarkeit, Integrität und Konsistenz der Systeme einschließlich der auf diesen Systemen gespeicherten und für Verarbeitungszwecke genutzten Daten, Programme und Prozeduren.

DoS-ATTACKE

Eine künstlich herbeigeführte Überlastung eines Webservers oder Datennetzes – gesteuert von Cyberkriminellen. Im Gegensatz zu einer einfachen Denial-of-Service-Attacke („DoS“) haben Distributed-Denial-of-Service-Attacken („DDoS“) eine immense Schlagkraft. Mehrere Computer greifen dabei gleichzeitig und im Verbund („Botnetze“) eine Webseite oder eine ganze Netzinfrastruktur an. Dies kann sehr schnell zum Ausfall der Server führen.

E.

ENTSCHLÜSSELUNG

Vorgang, bei dem unter Verwendung mathematischer Algorithmen und privater oder geheimer Schlüssel elektronische Daten wieder les- bzw. verarbeitbar gemacht werden. In verschlüsselter Form sind die Daten von unbefugten Dritten nicht einsehbar. Die Daten können nur vom Besitzer des entsprechenden privaten oder geheimen Schlüssels wieder in die Originalform überführt werden.

F.

FUZZING

„Fuzzing“ ist eine automatisierte Testmethode für Software, bei der ein Programm eine Vielzahl automatisch generierter Eingabedaten verarbeiten muss, ohne dabei eine Fehlfunktion zu zeigen. Findet ein Hacker durch Fuzzing ein Eingabemuster, das eine Fehlfunktion erzeugt, muss überprüft werden, ob sich der gefundene Fehler als Sicherheitslücke ausnutzen lässt.

FAKE PRESIDENT

Bezeichnet eine Betrugsmethode („Enkeltrick“), bei welcher E-Mails mit angeblichen Transaktionsanordnungen bzw. Aufforderung zu bestimmten Handlungen im Namen des Firmenchefs an Mitarbeiter des Unternehmens geschickt werden. Diese Betrugsmethode kommt sehr häufig vor, weil die E-Mail-Adressen im Internet öffentlich zugänglich sind.

G.

GEHEIMER SCHLÜSSEL

Geheime Schlüssel werden im Zusammenhang mit symmetrischen Kryptoalgorithmen verwendet. Im Gegensatz zu den bei asymmetrischen Kryptoalgorithmen eingesetzten privaten Schlüsseln ist das gesamte Schlüsselmaterial allen Kommunikationspartnern bekannt.

H.

HTTPS

„HTTPS“ bzw. „Hypertext Transfer Protocol Secure“ ist ein Protokoll zur sicheren Datenübertragung im Internet. Beispielsweise wird es zur Kommunikation zwischen Webbrowser und Webserver verwendet. Bekannt ist die Buchstabenfolge „HTTPS“ den meisten aus der Adresszeile im Webbrowser: Hier wird sie vor jeder sicheren Webseite als „https://“ angezeigt. Die Verbindung wird über ein erworbenes SSL-Zertifikat sichergestellt.

HTTP

Das „Hypertext Transfer Protocol“ HTTP ist im Gegensatz zu HTTPS nicht verschlüsselt. Daten, die mit diesem Protokoll übertragen werden, können leicht von Dritten gelesen oder manipuliert werden. Wenn Sie schützenswerte Informationen über das Internet austauschen, ist eine verschlüsselte Verbindung (z. B. HTTPS) sehr empfehlenswert.

I.

IT-FORENSIK

Die „IT-Forensik“ befasst sich mit der Untersuchung, Analyse und Aufklärung von Sicherheitsvorfällen im Zusammenhang mit IT-Systemen.

K.

KEYLOGGER

Als „Keylogger“ wird Hard- oder Software zum Mitschneiden von Tastatureingaben bezeichnet. Sie zeichnen alle Tastatureingaben auf, um sie möglichst unbemerkt an einen Angreifer zu übermitteln. Dieser kann dann aus diesen Informationen für ihn wichtige Daten, wie z. B. Anmeldeinformationen oder Kreditkartennummern filtern.

KUMULATIONSEFFEKT IM IT-GRUNDSCHUTZ

Der Kumulationseffekt beschreibt, dass sich der Schutzbedarf eines IT-Systems erhöhen kann, wenn durch Kumulation mehrerer (z. B. kleinerer) Schäden auf einem IT-System ein insgesamt höherer Gesamtschaden entstehen kann. Ein Auslöser kann auch sein, dass mehrere IT-Anwendungen bzw. eine Vielzahl sensitiver Informationen auf einem IT-System verarbeitet werden, sodass durch Kumulation von Schäden der Gesamtschaden höher sein kann.

M.

MAN-IN-THE-MIDDLE-ANGRIFF

Ziel bei einem „Man-in-the-Middle-Angriff“ ist es, sich unbemerkt in eine Kommunikation zwischen zwei oder mehreren Partnern einzuschleichen, beispielsweise um Informationen mitzulesen oder zu manipulieren. Hierbei begibt sich der Angreifer „in die Mitte“ der Kommunikation, indem er sich gegenüber dem Sender als Empfänger und gegenüber dem Empfänger als Sender ausgibt.

N.

NICKNAPPING

Personen treten im Internet mit ihrem realen Namen oder unter der Verwendung eines Pseudonyms oder Nicknames auf. Als „Nicknapping“ bezeichnet man einen Cyberangriff, bei dem der Angreifer unter einem bekannten Namen oder Pseudonym auftritt. Dadurch versucht der Angreifer, gegenüber Dritten den Eindruck zu erwecken, er sei der eigentliche/ursprüngliche Inhaber des Namens oder des Pseudonyms. Gelingt dies, kann der Angreifer in begrenztem Maße als der eigentliche/ursprüngliche Inhaber agieren.

P.

PAIRING
Zwei bluetoothfähige Geräte wie z. B. Smartphone und Kopfhörer benötigen einen gemeinsamen Verbindungsschlüssel, um miteinander kommunizieren zu können. Dieser wird berechnet, nachdem auf beiden Geräten eine gleichlautende PIN eingegeben wurde. Die „besondere Vertrauensbeziehung“ zwischen den beiden Geräten bezeichnet man als „Pairing“.

PHARMING
Ist eine Betrugsmethode, die auf der Grundidee des Phishings beruht. Dabei wird der Benutzer durch die Nutzung von Systemmanipulationen auf gezielt gefälschte Webseiten umgeleitet, ohne dass er dies bemerkt. Dadurch ist es möglich, an persönliche Informationen wie z. B. Bankdaten zu gelangen.

PHISHING
Beim „Phishing“ wird z. B. mittels gefälschter E-Mails und/oder Webseiten versucht, Zugangsdaten für einen Dienst oder eine Webseite zu erlangen. Wird diese Manipulation vom Opfer nicht erkannt und die Authentizität einer Nachricht oder Webseite nicht hinterfragt, gibt das Opfer seine Zugangsdaten u. U. selbst unwissentlich in unberechtigte Hände.

R.

RANSOMWARE
Als „Ransomware“ werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (englisch: „ransom“) wieder freigegeben. Es handelt sich dabei um einen Angriff auf das Sicherheitsziel der Verfügbarkeit und eine Form digitaler Erpressung.

REPLAY-ANGRIFFE
„Replay-Angriffe“ beschreiben allgemein Angriffe, bei denen ein Informationsaustausch zuerst aufgezeichnet wird und die gewonnenen Informationen im Anschluss daran missbräuchlich wiederverwendet werden. Anhand eines aufgezeichneten Login-Vorgangs kann ein Angreifer beispielsweise versuchen, sich selbst unberechtigt Zugang zu dem jeweiligen System zu verschaffen.

S.

SANITARISIERUNG
Die Bereinigung einer Meldung von schutzbedürftigen Informationsanteilen. Ziel ist die Wahrung der berechtigten Schutzinteressen der am Informationsaustausch Beteiligten bei gleichzeitigem Erhalt der relevanten Informationen.

SCHADFUNKTION
Mit Schadfunktion wird eine vom Anwender ungewünschte Funktion bezeichnet, die die Informationssicherheit unbeabsichtigt oder bewusst gesteuert gefährden kann.

SCAREWARE

„Scareware“ ist eine Form von Schadsoftware, die der Nutzer selbst auf seinem System installiert. In den meisten Fällen wird dem Nutzer beim Surfen im Internet durch Täuschung oder Ausnutzen von technischem Unverständnis suggeriert, dass ein Problem mit seinem Computer besteht. Häufig wird dazu eine Infektion mit Schadsoftware gemeldet, eine angebliche Fehlfunktion des Betriebssystems erkannt oder mit einem wichtigen Sicherheits-Update geworben. Vertraut ein Anwender auf diese Meldungen und installiert die angebotene Software, hat er selbst dadurch das System im ungünstigsten Fall mit einer Schadsoftware infiziert.

SPOOFING

„Spoofing“ (englisch: „to spoof“, zu Deutsch: manipulieren, verschleiern oder vortäuschen) nennt man in der Informationstechnik verschiedene Täuschungsversuche zur Verschleierung der eigenen Identität und zum Fälschen übertragener Daten. Das Ziel besteht darin, die Integrität und Authentizität der Informationsverarbeitung zu untergraben.

SPYWARE

Als „Spyware“ werden Programme bezeichnet, die heimlich, also ohne darauf hinzuweisen, Informationen über einen Benutzer bzw. die Nutzung eines Rechners sammeln und an den Urheber der Spyware weiterleiten. Spyware gilt häufig nur als lästig, es sollte aber nicht übersehen werden, dass durch Spyware auch sicherheitsrelevante Informationen wie Passwörter ausgeforscht werden können.

T.

TROJANISCHES PFERD

Ein „trojanisches Pferd“, oft auch (fälschlicherweise) kurz „Trojaner“ genannt, ist ein Programm mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung. Ein trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogramms für seine Installation durch den Benutzer.

TLS (TRANSPORT LAYER SECURITY)

„SSL“ ist ein hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet. SSL wurde nach der Version 3.0 unter dem neuen Namen TLS „Transport Layer Security“ weiterentwickelt. Das „SSL-Protokoll“ stellt auf der Transportschicht einen sicheren „Tunnel“ zwischen Sender und Empfänger her, durch den die transportierten Daten gegen Kenntnisnahme und Veränderung geschützt werden.

V.

VERTEILUNGSEFFEKT
Der „Verteilungseffekt“ kann sich auf den Schutzbedarf relativierend auswirken, wenn zwar eine Anwendung einen hohen Schutzbedarf besitzt, ihn aber deshalb nicht auf ein betrachtetes IT-System überträgt, weil auf diesem IT-System nur unwesentliche Teilbereiche der Anwendung laufen.

VIREN
Klassische Form von Schadsoftware, die sich selbst verbreitet und unterschiedliches Schadpotenzial in sich tragen kann (keine Schadfunktion bis hin zum Löschen der Daten auf einer Festplatte). „Viren“ treten in Kombination mit einem Wirt auf, z. B. einem infizierten Dokument oder Programm.

Z.

ZERO-DAY-EXPLOIT
Die Ausnutzung einer Schwachstelle, die nur dem Entdecker bekannt ist, charakterisiert man mit dem Begriff „Zero-Day-Exploit“. Die Öffentlichkeit und der Hersteller des betroffenen Produkts merken in der Regel erst dann die Schwachstelle, wenn Angriffe entdeckt werden, die auf dieser Schwachstelle basieren. Der Hersteller hat keine Zeit, die Nutzer vor den ersten Angriffen zu schützen.

ZUGRIFF
Bezeichnet die Nutzung von Informationen bzw. Daten. Über Zugriffsberechtigungen wird geregelt, welche Personen oder IT-Anwendungen bevollmächtigt sind, Informationen oder Daten zu nutzen oder Transaktionen auszuführen.

VHV CYBERPROTECT

Die IT-Versicherung der VHV schützt Ihren Betrieb umfassend vor Schäden an Computersystemen und digitalen Archiven – bei technischen Defekten, kriminellen Angriffen von außen oder Untreue der eigenen Mitarbeiter.

Optimaler Schutz bei Hackerangriffen
Unser Produkt schützt Sie gegen Best Practices der Hacker und versichert Sie gegen durch Informationssicherheitsverletzung verursachte Vermögensschäden.

Auch bei nicht gezielten Angriffen
VHV CYBERPROTECT hilft sowohl bei gezielten als auch bei nicht gezielten Angriffen auf Ihr Unternehmen, z. B. gegen Schadsoftware, DDoS-Angriffe, unberechtigte Aneignung von Zugangscodes sowie Computer-Sabotage.

VHV Soforthilfe
Die IT-Experten stehen Ihnen rund um die Uhr an 365 Tagen telefonisch und persönlich zur Verfügung, damit Ihr Geschäftsbetrieb schnellstmöglich wieder aufgenommen werden kann.

Inklusive Drittschäden
Falls Dritte Ihnen gegenüber aufgrund einer Informationssicherheitsverletzung Schadenersatzansprüche geltend machen, sorgen wir für die Abwehr unberechtigter und die Erfüllung berechtigter Ansprüche.

Quellen: Bundesamt für Sicherheit der Informationstechnik und VHV Versicherungen

VHV CYBERPROTECT – RUNDUMSCHUTZ GEGEN IT-ANGRIFFE!

400.0031.56 Stand 03.2018 Druck 03.2018

CYBER

CYBERPROTECT

PRODUKTÜBERSICHT

	CYBERPROTECT
VHV SOFORTHILFE	
• 24 Stunden täglich / 365 Tage im Jahr	●
• Assistance-Hotline für Schadenmeldung / rund um die Uhr / sieben Tage die Woche	●
• Zeitnahe Feststellung des Sachverhalts	●
• Vermittlung von Erste-Hilfe-Dienstleister bei Cyberangriff oder zur Abwehr eines drohenden Cyberangriffs	●
• Kostenfrei für versicherte Risiken	●
Leistungen	
Bedarfsgerechter Deckungsumfang für kleine, mittlere und große Unternehmen	●
Flexibler Selbstbehalt / mind. 500 Euro	●
Weltweiter Geltungsbereich	●
Mitversicherte Personen (je nach Risiko)	
Gesetzliche Vertreter / Repräsentanten	●
Betriebsangehörige / Mitarbeiter	●
Freie im Auftrag und Namen der Firma tätige Mitarbeiter	●
Versicherte Risiken	
EIGENSCHÄDEN	
Ersatz von eigenen Vermögensschäden im Falle	
• der Wiederherstellungskosten von Daten und Software	●
• eines Ertragsausfalls nach Cyberangriff (Betriebsunterbrechung) / Selbstbehalt frei wählbar (12, 24 oder 48 Stunden)	●
• von Bußgeldern wegen Datenschutzverletzungen im Ausland (sofern rechtlich möglich)	●
• von Telefonkosten bei Missbrauch der digitalen Telefonanlage durch Dritte	●
Cyber-Spionage	○
Vertrauensschaden	○
HAFTPFLICHT	
Prüfung der Haftpflichtfrage	●
Abwehr unberechtigter Ansprüche	●
Freistellung von Schadenersatzansprüchen	
• aufgrund rechtswidriger digitaler Kommunikation	●
• aus Vertragserfüllung oder Verzögerung der Leistung	●
Strafrechtsschutz / Verteidigungskosten aus einem Ordnungswidrigkeiten- oder Strafverfahren gegen den Versicherungsnehmer	●
Ausgleich von Vertragsstrafen aus Verletzung von PCI-Standards	○
D&O-Absicherung	○

VHV VERSICHERUNGEN

VON EXPERTEN VERSICHERT

	CYBERPROTECT
SERVICE UND KOSTEN	
Forensische Untersuchungen zur Feststellung eines Cyberangriffs und	
• zur Ermittlung der Ursachen	●
• zur Feststellung des Schadens	●
• zu Empfehlungen zur Vorbeugung oder Reaktion	●
Benachrichtigungskosten von Betroffenen und Datenschutzbehörden bei Datenschutzverletzungen, inkl. Callcenter-Kosten	●
Kosten für Öffentlichkeitsarbeit	●
Kosten für PR-Beratung	●
Kosten für die Überwachung von Kreditkarten oder sonstigen Bankkonten im Falle des Verlustes solcher Daten	●
Aufwendungen vor Eintritt des Versicherungsfalls	●
Versicherte Risikoszenarien (Beispiele)	
Cyberangriff (gezielt/nicht gezielt) / (Distributed-)Denial-of-Service-Attacke (DDoS/DoS) / Kreditkartenmissbrauch / Befall durch Computer-Viren / Unberechtigter Zugriff auf Daten durch Cyber-Spione / Schädigung des IT-Systems durch Mitarbeiter / Gehackte Telefonanlage / Hilfe bei Erpressung	●

Die Produktbeschreibungen beziehen sich auf den Leistungsumfang unseres derzeit aktuellen Produkts aus 01/2018 und sind stark verkürzt wiedergegeben. Maßgebend ist ausschließlich der Wortlaut der Versicherungsbedingungen.

● enthalten ○ optional

UNSERE LEISTUNGEN AUF DEN PUNKT GEBRACHT.

OPTIMALER SCHUTZ BEI HACKERANGRIFFEN

Unser Produkt schützt Sie gegen Best Practices der Hacker und versichert Sie gegen durch Informationssicherheitsverletzung verursachten Vermögensschäden.

AUCH BEI NICHT GEZIELTEN ANGRIFFEN

VHV CYBERPROTECT hilft sowohl bei gezielten als auch bei nicht gezielten Angriffen auf Ihr Unternehmen. Dadurch sind Sie z. B. gegen Schadsoftware, DDoS-Angriffe, unberechtigte Aneignung von Zugangscodes sowie Computersabotage abgesichert.

VHV SOFORTHILFE

Die VHV Soforthilfe sorgt für kompetente Hilfe – bei Bedarf auch vor Ort. Hierzu wird Ihnen rund um die Uhr an 365 Tagen im Jahr geholfen. Die IT-Experten stehen Ihnen telefonisch und persönlich zur Verfügung, damit Ihr Geschäftsbetrieb schnellstmöglich wieder aufgenommen werden kann.

INKLUSIVE DRITTSCHÄDEN

Falls Dritte Ihnen gegenüber aufgrund einer Informationssicherheitsverletzung Schadenersatzansprüche geltend machen, sorgen wir für die Abwehr unberechtigter und die Erfüllung berechtigter Ansprüche.

GUT ZU WISSEN

Ab 25.05.2018 gilt für alle Unternehmen, die personenbezogene Daten verarbeiten, die neue EU-Datenschutz-Grundverordnung (EU-DSGVO). Im Falle einer Datenschutzverletzung drohen den Firmen Haftpflichtansprüche der betroffenen Kunden. Auch hier sorgt VHV CYBERPROTECT im Versicherungsfall für die Abwehr unberechtigter und die Erfüllung berechtigter Ansprüche.

**IHR VHV PARTNER HILFT IHNEN GERN WEITER.
ODER RUFEN SIE UNS EINFACH AN.**

**INFOTELEFON: 0511.907-38 38
ODER E-MAIL AN CYBER@VHV.DE**

**VHV Versicherungen
30138 Hannover
vhv.de**

400.0031.45 Stand 01.2018 Druck 01.2018

CYBER

CYBERPROTECT

VHV VERSICHERUNGEN

VON EXPERTEN VERSICHERT

EFFEKTIVER SCHUTZ VOR DIGITALEN GEFAHREN.

Digitales Arbeiten und die tägliche Nutzung von E-Mails sind heute selbstverständlich. Die Sicherheit von Daten und IT-Systemen ist dabei entscheidend. Doch jedes vierte mittelständische Unternehmen in Deutschland ist bereits Opfer eines Angriffs auf die eigene IT-Infrastruktur geworden – Tendenz steigend. Der finanzielle Schaden beträgt dabei durchschnittlich über 40.000 Euro. Ob sogenannte Denial-of-Service-Attacken, die ganze IT-Infrastrukturen lahmlegen, Betrugsmaschen wie „Fake President" oder der Missbrauch sensibler Daten durch ausgeschiedene Arbeitnehmer – die IT-Landschaft ist ein Einfallstor für Kriminelle, die Ihren unternehmerischen Erfolg bedrohen. VHV CYBERPROTECT schützt Sie vor den finanziellen Folgen eines Cyberschadens und ersetzt Vermögensschäden, die sich aus Informationssicherheitsverletzungen ergeben.

VHV CYBERPROTECT leistet umfassenden Schutz bei Eigenschäden – also dann, wenn Sie selbst betroffen sind. Aber auch Haftpflichtansprüche Dritter werden übernommen. Zum Beispiel, wenn Sie gehackt wurden und sensible Daten Ihrer Kunden in die Hände von Betrügern geraten sind, die diese für weitere Betrugsmaschen nutzen. Im Schadenfall können Sie sich auf ein umfassendes Krisenmanagement verlassen. Auf Wunsch behebt unser zertifizierter IT-Dienstleister den Schaden schnellstmöglich, sorgt für forensische Untersuchungen der betroffenen Technik und kümmert sich bei Bedarf auch um eine PR-Beratung, falls Sie die Öffentlichkeit über eine Datenschutzverletzung informieren müssen.

Als Auditor prüft er abschließend, ob Ihre IT-Sicherheit wiederhergestellt ist. Selbstverständlich sind Sie nicht an unsere IT-Spezialisten gebunden. Wir übernehmen auch die Aufwände fremder Dienstleister. Und dank der Leistungs-Update-Garantie können Sie sicher sein, dass Ihr Versicherungsschutz langfristig auf dem neuesten Stand bleibt.

Hier drohen Cyberschäden

Cyberrisiken drohen in praktisch allen digitalisierten Prozessen eines Unternehmens:

- Verwaltung, Einkauf, Auftragsverarbeitung
- Planung, Abwicklung
- in allen Bereichen, in denen personenbezogene oder anderweitig sensible Daten verarbeitet werden

Was ist abgesichert?

Ist durch einen Hackerangriff die Integrität, Vertraulichkeit und Verfügbarkeit der Daten nicht mehr gewährleistet, übernimmt VHV CYBERPROTECT den entstandenen Vermögensschaden, wie zum Beispiel:

- Wiederherstellungskosten von Daten und Software inklusive Kosten für Neuinstallation und Einrichtung
- Übernahme von Schadenersatzansprüchen
- Übernahme von Serviceleistungen, zum Beispiel Soforthilfe, Krisenmanagement oder PR-Beratung nach Reputationsverlust

UNSERE STARKEN LEISTUNGEN:

1 UMFASSENDES PRODUKT
2 INDIVIDUELLE ZUSATZLEISTUNGEN
3 VHV SOFORTHILFE
4 LEISTUNGS-UPDATE-GARANTIE
5 JEDERZEIT KÜNDBAR

IHR VHV PARTNER HILFT IHNEN GERN WEITER.
ODER RUFEN SIE UNS EINFACH AN.
INFOTELEFON: 0511.907-38 38
ODER E-MAIL AN CYBER@VHV.DE

IHRE VHV CYBERVERSICHERUNG:

Individuelle Zusatzleistungen

VHV Soforthilfe

Leistungs-Update-Garantie

CYBERPROTECT

1 UMFASSENDES PRODUKT

Mit VHV CYBERPROTECT können Sie sich auf einen besonders umfassenden Versicherungsschutz verlassen. Davon profitieren Sie bereits beim Vertragsabschluss: Die Police beinhaltet eine individuelle Rückwärtsversicherung. Denn eine Infektion erkennt man durchschnittlich erst nach rund 470 Tagen, nachdem zum Beispiel ein Virus einen Rechner befallen hat. Mit vielen weiteren Details dieser Cyberversicherung schützen Sie Ihr Unternehmen – und damit die Basis Ihres Erfolgs.

Weltweiter Versicherungsschutz

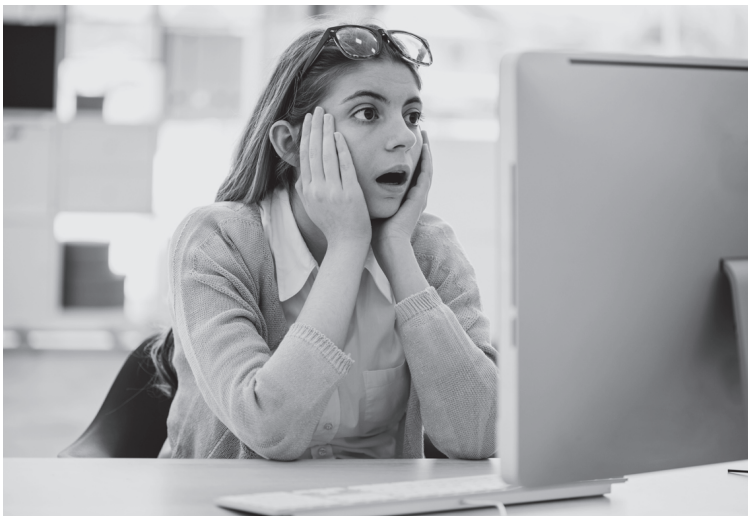
Das Internet kennt keine Grenzen. Deshalb sind Cyberrisiken international. Mit VHV CYBERPROTECT sichern Sie sich einen weltweiten Schutz nach deutschem oder europäischem Recht. Je nach Geschäftsgebiet können Sie individuell auch ein anderes Landesrecht vereinbaren – mit Ausnahme des Landesrechts der USA oder Kanada.

Umfangreicher Schutz bei Eigenschäden

Nach einem IT-Schaden wollen Sie eigentlich nur eines: Gewissheit, dass alles wieder läuft. Diese Sicherheit gibt Ihnen VHV CYBERPROTECT. Denn damit sichern Sie sich nicht nur die Kostenübernahme für die Widerherstellung von Daten und Software, sondern bekommen auch die Kosten für eine schnelle Einrichtung und Installation erstattet. Und wenn Ihr Geschäft nach einem Cyberangriff ruhen muss? Kein Problem, VHV CYBERPROTECT ersetzt den Schaden durch Betriebsunterbrechung oder Ertragsausfall.

Umfangreicher Haftpflichtschutz

Sobald Sie mit sensiblen Daten Dritter arbeiten, können daraus Haftpflichtrisiken entstehen. Zum Beispiel dann, wenn Sie infolge eines Hackerangriffs nicht produzieren können und Auftragnehmer auf die bestellte Ware warten müssen. Oder dann, wenn Ihre Daten unrechtmäßig missbraucht oder rechtswidrig veröffentlicht werden und daraus Ersatzansprüche gegen Sie gestellt werden. Wir prüfen Ansprüche gegen Sie eingehend und wehren unberechtigte Ansprüche ab. Berechtigte Schadenersatzansprüche – zum Beispiel wegen rechtswidriger digitaler Kommunikation oder einer verzögerten Lieferung regulieren wir sofort. So schützt VHV CYBERPROTECT nicht nur Ihre Daten, sondern auch Ihre Kunden- und Geschäftsbeziehungen.



Service und Kosten

Mit der Eliminierung der Infektion ist ein IT-Schaden oft noch nicht behoben. Meist schließen sich umfangreiche Arbeiten von IT-Spezialisten an: Oft muss die gesamte Software inklusive aller Daten wiederhergestellt werden. Parallel prüfen Forensiker, welche IT-Lücken zum Schaden geführt haben und welche Daten eventuell an die Hacker gegangen sind. All diese Arbeiten verursachen Kosten, für die VHV CYBERPROTECT einsteht.

Umfassender mitversicherter Personenkreis

Ob aus betrügerischer Absicht oder Versehen: Jede am Unternehmen beteiligte Person kann einen Cyberschaden verursachen. Deshalb sind bei VHV CYBERPROTECT auch praktisch alle Betriebsangehörigen sowie ehemalige Mitarbeiter mitversichert. Anders als bei anderen Versicherern sind zum Beispiel Abteilungsleiter automatisch mitversichert. Darüber hinaus deckt VHV CYBERPROTECT auch alle Schäden ab, die zum Beispiel durch freie Mitarbeiter oder andere im Auftrag und Namen der Firma tätige Mitarbeiter entstehen.

2 INDIVIDUELLE ZUSATZLEISTUNGEN

Sie wollen mehr als eine zuverlässige Basisabsicherung gegen Cyberschäden? Kein Problem. Mit unserer individuellen Zusatzabsicherung schützen Sie sich umfassend. Zum Beispiel vor speziellen Betrugsmaschen, die unter anderem Insider begehen könnten. Oder Sie begrenzen Ihre persönliche Haftung im Schadenfall mit einer speziellen Manager-Deckung.

Darüber hinaus können Sie sich mit Zusatzleistungen auch vor Vertragsstrafen wegen Verletzung von PCI-Standards im elektronischen Zahlungsverkehr sowie vor Cyberspionage schützen.

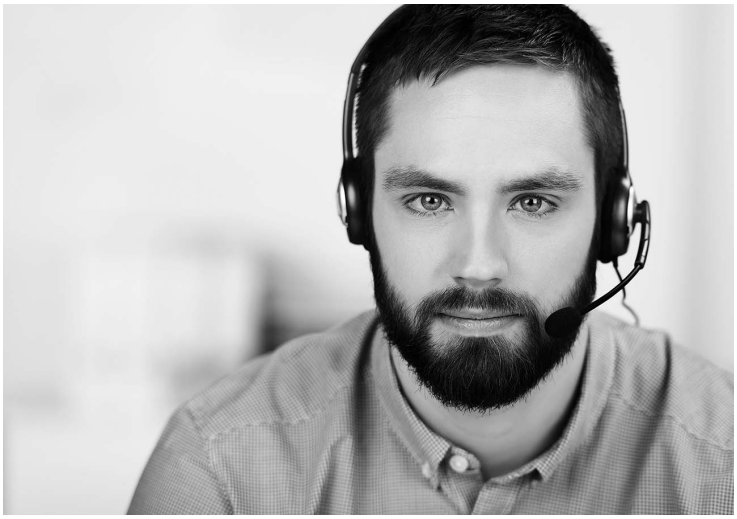
Vertrauensschaden

Ihre Mitarbeiter genießen Ihr volles Vertrauen. Kommt es zur Trennung, können diese ihr Insider-Wissen leicht gegen Sie einsetzen und zum Beispiel wichtige Daten vom Server löschen. Andere Cyberkriminelle nutzen mit der Betrugsmasche „Fake President“ das Vertrauen Ihrer aktiven Belegschaft aus. Dabei senden Hacker in Ihrem Namen eine E-Mail zum Beispiel an Ihre Buchhaltung und verlangen darin eine Geldüberweisung mit höchster Diskretion. Als zuverlässiger Mitarbeiter wird Ihr Finanzbuchhalter diesen Auftrag natürlich sofort ausführen – und den Schaden mitunter erst bei der nächsten Bilanz feststellen. Anders als bei vielen anderen Versicherungen sind solche und andere Schäden, auch durch ausgeschiedene Mitarbeiter, bei VHV CYBERPROTECT automatisch mitversichert.

D&O-Absicherung

D&O steht für „Directors and Officers“. Diese Absicherung umfasst einen speziellen Haftpflichtschutz für die Geschäftsführung. Denn als Geschäftsführer haften Sie bei einer Verletzung der Informationssicherheit mit Ihrem privaten Vermögen. Bei VHV CYBERPROTECT sind Sie und Ihr gesamtes Führungsteam umfassend abgesichert.

SOFORT BEREIT. WENN HILFE NICHT WARTEN KANN.



GUT ZU WISSEN

Ob einfaches Bonusprogramm oder vertrauliche Informationen Ihrer Kunden: Für alle Unternehmen, die personenbezogene Daten verarbeiten, gilt ab Mai 2018 die neue EU-Datenschutz-Grundverordnung (EU-DSGVO). Im Falle einer Verletzung drohen den Firmen Haftpflichtansprüche. Verstöße gegen die EU-DSGVO werden mit Bußgeldern von bis zu 2 % bzw. 4 % des gesamten, weltweit erzielten Jahresumsatzes des Unternehmens geahndet.

Gerade deshalb ist es wichtig, sich um die IT-Sicherheit im Unternehmen zu kümmern und sich vor den finanziellen Folgen eines Schadens zu schützen – zum Beispiel mit VHV CYBERPROTECT.

3 VHV SOFORTHILFE

Tempo entscheidet nach einem Cyberschaden. Deshalb ist in VHV CYBERPROTECT ein Soforthilfe-Programm integriert, das Ihnen im Schadenfall einen zertifizierten IT-Dienstleister und Auditor zur Seite stellt. Dieser ist 365 Tage im Jahr rund um die Uhr erreichbar, um einen Schaden aufzunehmen und erste Beratung zu geben. Danach stellt er zügig den Sachverhalt fest und organisiert eine Reparatur vor Ort. Und weil Unternehmen nach einem IT-Schaden unter Umständen verpflichtet sind, die Öffentlichkeit zu informieren, organisiert er auch eine professionelle PR-Beratung. Zum Schluss stellt der Auditor die Sicherheit Ihrer IT-Landschaft fest, dokumentiert diese und berät Sie zur effektiven Abwehr zukünftiger Angriffe.

4 LEISTUNGS-UPDATE-GARANTIE

Wir entwickeln unsere Produkte stetig weiter. Damit Sie langfristig und automatisch in den Genuss dieser Updates kommen, bieten wir eine Leistungs-Update-Garantie. Damit wird Ihr bestehender Versicherungsschutz immer auf den neuesten Stand gebracht und Sie erhalten automatisch die neuen, verbesserten Leistungen. Das Beste daran: Es kostet Sie keinen Cent mehr. Übrigens: Die Leistungs-Update-Garantie gilt auch für unsere individuell vereinbarten Zusatzleistungen.

5 JEDERZEIT KÜNDBAR

Das Risiko von IT-Schäden wächst, entsprechend gibt es immer neue Cyberversicherungen am Markt. Wir wollen diese nicht mit immer günstigeren Preisen unterbieten, sondern Sie langfristig mit Leistung überzeugen. Deshalb verzichten wir auf lange unkündbare Laufzeiten. Wenn Sie sich für einen anderen Anbieter entscheiden, können Sie jederzeit ganz einfach kündigen.

Gut, wenn man versichert ist.
Besser, wenn man von Experten versichert ist.

Die Informationstechnologie ist allgegenwärtiger Bestandteil Ihres beruflichen Alltags. Durch den Umgang damit entstehen hohe Risiken außerhalb Ihres eigentlichen Geschäftsfelds. Diese gefährden die Verfügbarkeit, die Integrität und Vertraulichkeit von Daten – und damit die geforderte Informationssicherheit. Dadurch drohen Vermögensschäden. VHV CYBERPROTECT schützt Sie als Unternehmer vor diesen Risiken und Gefahren. Umfassend. Zuverlässig. Und mit starken Leistungen.

Darüber hinaus können Sie auf unsere Fairness vertrauen. Und als faire Experten sind wir verpflichtet, darauf hinzuweisen, dass die Produkt- und Leistungsbeschreibungen in dieser Broschüre verkürzt wiedergegeben sind und ausschließlich der Wortlaut der Versicherungsbedingungen maßgebend ist.

AUF WIEDERSEHEN BEI IHREM VHV PARTNER.

VHV Versicherungen
30138 Hannover
vhv.de

400.0031.46 Stand 03.2018 Druck 03.2018