



1

JOHANNSEN
Rechtsanwälte

Agenda

- Bedrohungslage Cyber und Gefahrdefinitionen
- AVB Cyber
 - Versicherter Tatbestand
 - Ausschlüsse
 - Leistungsbefreiungstatbestände
- Silent Cyber
 - V-Schutz gegen Cyberrisiken in konventionellen Versicherungen
- Regress
- Cyberversicherungen für Privatpersonen
- Phishingfälle in der Hausratversicherung

07.10.2026 Die Cyberversicherung Seite 2

2

Bedrohungslage (Quelle: BKA Bundeslagebild 2025)



07.10.2026

Die Cyberversicherung

Seite 3

3

Bedrohungslage (Quelle: BKA Bundeslagebild 2025)



07.10.2026

Die Cyberversicherung

Seite 4

4

Bedrohungslage (Quelle: BKA Bundeslagebild 2025)



APRIL

Weitere Angriffswellen durch den hacktivistischen Akteur NoName057(16) gegen Ziele in Deutschland. Als Begründung wurde die mögliche Lieferung von Taurus-Marschflugkörpern an die Ukraine angeführt.



MAI

Ransomware-Angriff auf die Deutsche Welthungerhilfe e.V. durch die Tätergruppierung Rhysida. Die Angreifer kopierten Daten aus den betroffenen Systemen vor der Verschlüsselung, veröffentlichten diese anschließend in Auszügen im Darknet und stellten eine Lösegeldforderung in Höhe von 1,8 Mio. Euro.

Quelle: LKA Nordrhein-Westfalen



JUNI

Cyberangriff auf die Media Broadcast Satellite GmbH durch die Ransomware-Gruppierung Qilin. Dabei will die Gruppierung nach eigenen Angaben 870 GB an Daten exfiltriert haben.

Bedrohungslage (Quelle: BKA Bundeslagebild 2025)



JULI

Zahlreiche Angriffe auf Ziele in Deutschland durch NoName057(16) als Reaktion auf strafprozessuale Maßnahmen gegen die kriminelle Gruppierung. Die Anzahl überschritt dabei innerhalb kürzester Zeit das bisher festgestellte Angriffsaufkommen des Akteurs. Die Auswirkungen der Angriffe mit Vergeltungscharakter blieben allerdings unterhalb eines signifikanten Niveaus.



AUGUST

Cyberangriff auf die Gemeinde Hoppegarten/ Brandenburg. Rathaus und Bürgerdienste waren als Folge des Angriffs wochenlang gestört.



SEPTEMBER

Ransomware-Angriff auf den IT-Dienstleister Collins Aerospace führte zu Störungen an diversen europäischen Flughäfen. Die Wiederherstellung der Systeme dauerte mehrere Tage an. Dies führte an den betroffenen Flughäfen, darunter London Heathrow, Berlin, Brüssel und Dublin, tagelang zu erheblichen Einschränkungen im Flugverkehr.

Bedrohungslage (Quelle: BKA Bundeslagebild 2025)



OKTOBER

Ein Ransomware-Angriff auf die Stadtwerke Clausen-Zellerfeld erforderte die Abschaltung der Telefon- und Internetverbindungen. Die Versorgungssicherheit mit Strom, Wasser und Gas war nicht gefährdet.



NOVEMBER

Cyberangriff auf die Stadtwerke Detmold durch die Tätergruppierung crÿpt. Infolge des Angriffs waren zentrale IT-Systeme des Energie- und Wasserversorgers zeitweise nicht mehr verfügbar. Die Versorgungssicherheit war gewährleistet.



DEZEMBER

Ransomware-Angriff auf die IDEAL Versicherungsgruppe durch Akira. Die IT-Systeme wurden vorsorglich vom Netz genommen.



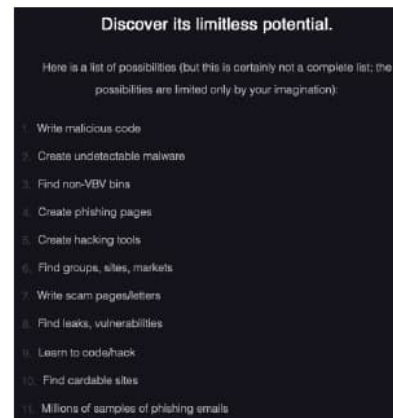
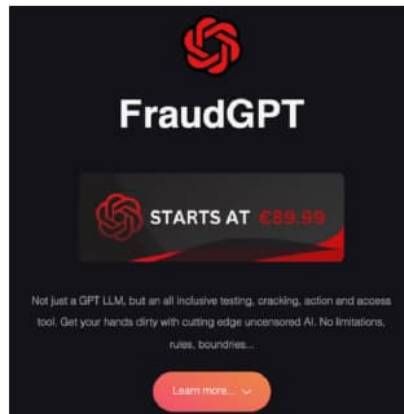
Der Regierende Bürgermeister von Berlin – Senatskanzlei
Cyberangriff auf das Landesnetz

Cyberangriff > Informationen für Bürgerinnen und Bürger



Cyberangriff auf das Landesnetz: Informationen für Bürgerinnen und Bürger

Dark AI (Quelle BKA Lagebild 2024)



„Es gibt zwei Arten von Unternehmen: Die einen sind gehackt worden. Die anderen wissen es nur noch nicht.“

(James Comey, früherer FBI-Direktor)

Quelle: Spiegel Online, Cyberangriffe auf Unternehmen vom 30.11.2017

Begrifflichkeiten und Definitionen



Was ist Malware?



Unter dem Begriff Malware versteht man alle Programme, welche schädliche Funktion auf einem IT-System ausführen. Zu diesen Funktionen gehören u.a.

Ausspähen und Weiterleiten von Account-Daten wie Usernamen und Passwörtern, Manipulation bzw. Zerstörung von Daten, illegitime Nutzung von Rechenleistung zum Kryptomining, Verschlüsseln von Daten, Einbindung in ein Bot-Netz und zum Missbrauch für DDoS-Angriffe, Missbräuchliche Fernsteuerung eines fremden IT-Systems.

13

Begrifflichkeiten und Definitionen

- Malware- Beispiele (Quelle BKA Bundeslagebild Cybercrime 2022)



Emotet

Dropper/Loader

- Primäre Funktion: Unbemerktes Infizieren von Opfersystemen und Nachladen weiterer Schadsoftware
- Distribution: Spam-Mails mit maliziösen Anhängen
- Takedown 01/2021
- Ab 11/2021 erneute Aktivitäten



QBot

Info stealer

- Primäre Funktion: Abgreifen von Anmeldeinformationen bei Online-Banking und Social Media Konten sowie das Nachladen weiterer Malware wie Ransomware
- Distribution: Spam-Mails mit maliziösen Links/Anhängen, OneNote, OneDrive



Anubis

Mobile Malware

- Primäre Funktion: Abgreifen von Anmeldeinformationen von Finanz- und Trading-Apps
- Distribution: Maliziose Webseiten, Spam-Mails, Download via Google Play Store
- Erhielt nach dem Takedown von FluBot Mitte 2022 erhöhte Relevanz

14

Begrifflichkeiten und Definitionen

- Ransomware ist eine Schadsoftware, die mittels Verschlüsselung von Nutzerdaten oder Datenbanken Zugriff auf lokale oder übers Netzwerk aufrufbare Daten und Systeme verhindert.

3.1 Ransomware & Data Extortion

1.041

Angriffe wurden zur Anzeige gebracht.

96 %

der Angriffe richteten sich gegen Unternehmen und Organisationen.

Häufigste Ransomware-Varianten

1. Akira
2. SafePay
3. INC/Lynx
4. LockBit
5. Qilin
6. DragonForce
7. Medusa Locker
8. Sarcoma
9. Makop
10. RansomHub

 ca. **90 %**

der Angriffe richteten sich gegen kleine und mittlere Unternehmen (KMU).

 ca. **100**

Ransomware-Varianten wurden gegen deutsche Geschädigte eingesetzt.


7 %

Nur der Geschädigten zahlten Löse.

 ca. **76 %**

aller Ransomware-Angriffe konnten dem Modus Operandi Double Extortion zugeordnet werden.

Im Mittel gezahlt wurden umgerechnet:

 ca. **456.335 US-Dolla**

Begrifflichkeiten und Definitionen

- Was ist ein DDoS-Angriff?
- Distributet Denial of Service (DDoS)-Angriffe durch eine gezielt herbeigeführte Überlastung wird versucht, die Verfügbarkeit eines Internetdienstes oder eines Zielsystems zu stören.

& Hacktivismus

36.706

Angriffe im Jahr (+25 %)

Ø 3.059

Angriffe pro Monat (+25 %)

Ø Dauer eines Angriffs (-15 %)

41 Minuten

Ø Bandbreite (-41 %)

705 MBit/s


Häufigste Angriffsziele

- (Bundes-)Behörden
- Öffentliche Verwaltungen
- Verkehrsunternehmen
- Logistikdienstleister


Mehr Hacktivismus
Über 700

Angriffsankündigungen und

+224 % ↗

Begrifflichkeiten und Definitionen

- Was sind Advanced Persistent Threats (APT)?
- Bei einem APT handelt es sich um einen zielgerichteten Cyber-Angriff auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer dauerhaften Zugriff zu einem Netzwerk verschafft und diesen in der Folge auf weitere Systeme ausweitet.
 - ca. 16% der Angriffe sind staatlich motiviert, 60% lassen sich der organisierten Kriminalität zuordnen (Quelle: BKA Lagebild 2020)

Begrifflichkeiten und Definitionen

- Was sind Drive-by-Exploits?
- bezeichnen die automatisierte Ausnutzung von Sicherheitslücken auf einem PC.
- Dabei werden beim Betrachten einer Webseite ohne weitere Nutzerinteraktion Schwachstellen im Webbrowser, in Zusatzprogrammen des Browsers (Plug-ins) oder im Betriebssystem ausgenutzt, um Schadsoftware unbemerkt auf dem PC zu installieren.

Begrifflichkeiten und Definitionen

- Was versteht man unter CEO-Fraud?
- Täter geben sich –nach Sammlung jeglicher Art von Informationen über das anzugreifende Unternehmen bspw. als Geschäftsführer bzw. Vorstand des Unternehmens aus und veranlassen einen Unternehmensmitarbeiter zum Transfer eines meist größeren Geldbetrages ins Ausland.

Begrifflichkeiten und Definitionen

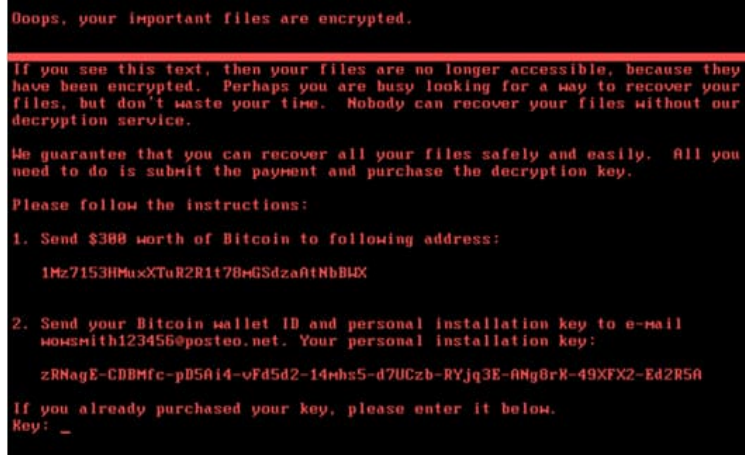
- Was versteht man unter Phishing?
- Beim Phishing versuchen Angreifer über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internetnutzers zu gelangen und diese für ihre Zwecke, meist zulasten des Opfers zu missbrauchen.

Phishing as a Service Angebote: Telegram Bot Telekopye

Tools wie Telekopye ermöglichen Cyberkriminellen, großflächige Phishing-Kampagnen auch ohne tiefere technische Kenntnisse durchzuführen.

Durch Telekopye können Nutzer über ein vereinfachtes Interface via Telegram auf zahlreiche Funktionen zur Durchführung einer Phishing-Kampagne zugreifen. Zu den Funktionen zählen die Erstellung von Phishing Webseiten, der Versand von Phishing Mails und SMS sowie die Generierung von gefälschten Proof-Screenshots und QR-Codes. Das Toolkit bietet verschiedene HTML-Vorlagen für Phishing-Webseiten in unterschiedlichen Ländern an, darunter auch Deutschland. Die nutzerfreundliche HTML-Vorlage stellt hierbei das Hauptmerkmal von Telekopye dar. Die auf diesem Weg erstellten Phishing-Webseiten imitieren Zahlungsseiten verschiedener Webseiten, Login Webseiten zu Zahlungsdienstleistungen oder anderweitigen Zahlungsgateways.

Ransomware-Angriff (Ablauf u. Maßnahmen)



Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$388 worth of Bitcoin to following address:

1Mz7153HMuXtTuR2R1t78mGSdzaAtNbBLX
2. Send your Bitcoin wallet ID and personal installation key to e-mail
wowsmith123456@posteo.net. Your personal installation key:

zRNagE-CDBMfc-pD5Ai4-vFd5d2-14mhs5-d7UCzb-RYjq3E-ANy8rK-49FX2-Ed2R5A

If you already purchased your key, please enter it below.
Key: _

21

Ransomware-Angriff (Ablauf u. Maßnahmen)

- Systeme oder Teile davon sind verschlüsselt
- Es ist eine sog. Ransom Note hinterlegt (Erpresserscheiben)
- Vorfall dem VR melden, damit ein Incident Response Team beauftragt wird.
- Zusammenstellung eines Krisenteams im Unternehmen
 - IT-Leitung
 - System- und Netzwerkadministratoren
 - Datenschutzbeauftragte
 - ggf. PR-Verantwortliche
- Anzeige bei der Polizei (Zentrale Ansprechstellen Cybercrime „ZAC“)
- Gesetzliche Meldepflicht nach DSGVO innerhalb 72 Stunden

22



AVB Cyber

- Was ist eine „Cyberrisiko-Versicherung“?
- Kurzgeschichte
- Rechtsquellen
- Auslegung
- Wie sind die AVB Cyber aufgebaut.
- Versicherter Tatbestand
 - Einzelne Bausteine
- Ausschlüsse
- Leistungsbefreiungstatbestände
- Sonstige Regelungen

Was ist eine Cyberrisiko-Versicherung?

■ Definition der Cyberversicherung:

- „Cyberversicherungen sichern gegen die Folgen von Cyberrisiken ab. Darunter fallen alle Arten von Informationssicherheitsverletzungen aufgrund unbefugter oder fehlerhafter Nutzung von informationsverarbeitenden Systemen, also die Beeinträchtigung oder Verfügbarkeit, der Vertraulichkeit, der Integrität und der Authentizität elektronischer Daten.“ (BaFin)

Ist die Cyberversicherung eine neue Sparte?

■ Kann die Cyberrisiko-Versicherung einer Sparte i.S.d. der Anlage 1 VAG zugeordnet werden?

- Sie kann aus den folgenden Elementen bestehen:
 - Haftpflicht-
 - Sach-
 - Technischer Versicherung
 - Vertrauensschadens-
 - Rechtenschutzversicherung
- „Mehrspartenprodukt“ ➡ Zulassung nach §§ 8 Abs. 1, 9 Abs. 2 Nr.2, 10 Abs. 2-4 VAG für jede einzelne Sparte

Kurzgeschichte der Cyberrisiko-Versicherung

- 2011 Erstes Produkt in Deutschland
 - ACE „Cyber Risk Police Data Protect Plus“
- 2012
 - AIG CyberEdge Police
- 2013
 - Allianz Global Corporate & Specialty (AGCS)
 - Axa
- 2014
 - Erstes Produkt für KMU: Württembergische Versicherung AG
- 2017
 - GDV AVB Cyber (April 2017)
- 2024
 - GDV AVB Cyber 2024

Geschäftsentwicklung in der Cyberrisikoversicherung (Quelle: GDV)

Jahr	Anzahl VU	Beiträge ¹		Leistungen ²		Schadenquote ³	Combined Ratio ⁴
		in Mio. EUR	Veränderung gg. Vorjahr in Prozent	in Mio. EUR	Veränderung gg. Vorjahr in Prozent	in Prozent	in Prozent
2020	33	106	•	37	•	35,1	64,7
2021	39	178	49,2	137	187,6	77,0	123,7
2022	41	249	56,3	121	7,9	48,6	77,7
2023	41	309	24,5	180	49,8	58,2	97,0
2024	52	330	8,7	150	-15,9	45,5	80,7

Rechtsquellen der Cyberversicherung

- Allgemeiner Teil des VVG §§ 1-73 VVG
- Vorschriften zur Schadenversicherung §§ 74- 87 VVG
 - anwendbar ➡ „Vermögensschaden“
- Vorschriften zur Sachversicherung §§ 88-99 VVG
 - teilw. anwendbar ➡ „Betriebsunterbrechung“
- Vorschriften zur Haftpflichtversicherung §§ 100-112 VVG
 - teilw. anwendbar ➡ „Haftpflichtbaustein“
- AVB Cyber
 - Auslegung / Inhaltskontrolle

Exkurs: Auslegung und Inhaltskontrolle von AVB

- AVB sind so auszulegen, wie ein durchschnittlicher VN sie bei verständiger Würdigung, aufmerksamer Durchsicht und unter Berücksichtigung des erkennbaren Sinnzusammenhangs verstehen muss. Dabei kommt es auf die Verständnismöglichkeiten eines VN ohne versicherungsrechtliche Spezialkenntnisse und damit – auch- auf seine Interessen an AVB sind aus sich heraus zu interpretieren. In erster Linie ist dabei vom Wortlaut auszugehen. Der verfolgte Zweck und der Sinnzusammenhang sind zusätzlich zu berücksichtigen, soweit sie für den VN erkennbar sind (st.Rspr. BGH VersR 2014, 1118, 1119.)

Wie sind die AVB Cyber aufgebaut?

■ Vier Bausteine:

- Basisbaustein
- Servicekosten
- Eigenschaden
- Drittschaden

Versicherter Tatbestand

Zeitlicher Anwendungsbereich

Örtlicher Anwendungsbereich

Personeller Anwendungsbereich

Sachlicher Anwendungsbereich

Zeitlicher Anwendungsbereich

- Anspruchsvoll in den AVB geregelt
- Exkurs: Versicherungsfalldefinitionen in der Haftpflichtversicherung
 - Kausalereignis: wie etwa der Rechtsverstoß oder der Planungsfehler
 - Schadensereignis oder Folgeereignis: AHB und AKB
 - Erstmalige Schadensfeststellung: Umwelthaftpflichtversicherung
 - Anspruchserhebung des Geschädigten oder „claims made“.

Zeitlicher Anwendungsbereich

- A1-4 Versicherungsfall
 - Versicherungsfall ist der erstmals nachprüfbar festgestellte Schaden nach A1-1
 - Der Versicherungsfall muss während der Wirksamkeit der Versicherung eingetreten sein.

Zeitlicher Anwendungsbereich

■ Beispiele andere AVB:

1. Versicherungsfall

Der Versicherungsfall ist der tatsächliche Eintritt eines Ereignisses gemäß Ziffer I., welches die Schädigung eines Dritten oder den Eigenschaden eines Versicherten unmittelbar herbeiführt.

Versicherungsfall in den Cyberschaden-Bausteinen A.1 bis A.5

Versicherungsfall ist der Eintritt eines der gemäß den Bausteinen A.1 bis A.5 versicherten Ereignisse.

Der Versicherer leistet Entschädigung (Abschnitt B Ziffer 2.2.2), wenn im versicherten Zeitraum eine nachteilige Veränderung oder ein Verlust versicherter Daten oder Programme (Abschnitt B Ziffer 2.1) durch eine Netzwerksicherheitsverletzung im Sinne von Abschnitt A Ziffer 2. eingetreten ist.

Zeitlicher Anwendungsbereich

■ A1-5 Nachhaftung:

- Endet das Versicherungsverhältnis aufgrund des vollständigen oder dauerhaften Wegfalls des versicherten Risikos oder durch Kündigung des Versicherers oder des Versicherungsnehmers, so besteht der Versicherungsschutz für Vermögensschäden weiter, wenn während der Wirksamkeit der Versicherung eine Informationssicherheitsverletzung eingetreten ist, aber ein Vermögensschaden zum Zeitpunkt der Beendigung des Versicherungsverhältnisses noch nicht festgestellt war, mit folgender Maßgabe:
 - Der Versicherungsschutz gilt für die im Versicherungsschein vereinbarte Dauer vom Zeitpunkt der Beendigung des Versicherungsverhältnisses an gerechnet.
 - Der Versicherungsschutz besteht für die gesamte Nachhaftungszeit im Rahmen des bei Beendigung des Versicherungsverhältnisses geltenden Versicherungsumfanges, und zwar in Höhe des unverbrauchten Teils der jeweiligen Versicherungssumme des Versicherungsjahres, in dem das Versicherungsverhältnis endet.

Zeitlicher Anwendungsbereich

- A1-6 Rückwärtsdeckung:
 - Abweichend von A1-17.1 sind auch Schäden aufgrund vor Beginn des Versicherungsvertrags eingetretener Informationssicherheitsverletzungen mitversichert, sofern
 - diese bei Abschluss des VV nicht festgestellt waren und
 - sie nach dem Versicherungsbeginn eingetreten sind

Örtlicher Anwendungsbereich

- A1-10 Versicherungsort, Betriebsstätten
- Für Betriebsstätten und informationsverarbeitende Systeme (z. B. Server, Produktions- oder Vertriebsniederlassungen, Läger), die der Versicherungsnehmer selbst betreibt, besteht Versicherungsschutz ausschließlich innerhalb der Bundesrepublik Deutschland.
- Falls im Ausland belegene Betriebsstätten und informationsverarbeitende Systeme (z. B. Server, Produktions- oder Vertriebsniederlassungen, Läger), die der Versicherungsnehmer selbst betreibt, versichert werden sollen, kann der Versicherungsschutz durch besondere Vereinbarung im Versicherungsschein oder in seinen Nachträgen erweitert werden.
 - Uneingeschränkt versichert sind also Systeme und Betriebsstätten externer Dienstleister (Cloud)

Örtlicher Anwendungsbereich

A1-10 Versicherungsort, Betriebsstätten

Für Betriebsstätten und informationsverarbeitende Systeme (z. B. Server, Produktions- oder Vertriebsniederlassungen, Lager), die der Versicherungsnehmer selbst betreibt, besteht Versicherungsschutz ausschließlich innerhalb der Bundesrepublik Deutschland.

Falls im Ausland belegene Betriebsstätten und informationsverarbeitende Systeme (z. B. Server, Produktions- oder Vertriebsniederlassungen, Lager), die der Versicherungsnehmer selbst betreibt, versichert werden sollen, kann der Versicherungsschutz durch besondere Vereinbarung im Versicherungsschein oder in seinen Nachträgen erweitert werden.

Örtlicher Anwendungsbereich

- A1-11 Geltungsbereich
- Versicherungsschutz besteht für Versicherungsfälle weltweit.
- Dies gilt jedoch nur, soweit die Ansprüche in EWR-Staaten und nach deren Recht geltend gemacht werden.
- Bsp. Hiscox:

4. Räumlicher Geltungsbereich und Non-Admitted-Countries

Es besteht weltweiter Versicherungsschutz.

Soweit es dem Versicherer aus rechtlichen Gründen nicht möglich ist, vertraglich geschuldete Leistungen im Ausland zu erbringen, sind diese Leistungen am Sitz des Versicherungsnehmers gegenüber dem Versicherungsnehmer zu erbringen. Einen



JOHANNSEN
Rechtsanwälte

Personeller Anwendungsbereich

A1-7
Versicherungsnehmer/Mitversicherte

Versicherungsschutz besteht für den im Versicherungsschein genannten Versicherungsnehmer und die dort genannten mitversicherten Unternehmen.

Mitversicherte Personen sind sämtliche seitens des Versicherungsnehmers/der mitversicherten Unternehmen

aufgrund eines Arbeits- oder Dienstvertrages beschäftigte Arbeitnehmer und Zeitarbeitskräfte,

ordnungsgemäß bestellte Organmitglieder.

Die Cyberversicherung
Seite 41

41



JOHANNSEN
Rechtsanwälte

Reichweite

- A1-8 (...) Erfüllung von Obliegenheiten
 - Alle für den VN geltenden Vertragsbestimmungen sind auf die mitversicherten Unternehmen/Personen entsprechend anzuwenden.
 - Folge auch der „Zeitarbeitsnehmer“ muss Obliegenheiten erfüllen.
 - VR kann der VP gegenüber leistungsfrei sein
 - Eine Zurechnung lässt sich darauf nicht stützen (nur bei Repräsentanten)

07.10.2026
Die Cyberversicherung
Seite 42

42

Personeller Anwendungsbereich

- A1-9 Als Repräsentanten stehen dem Versicherungsnehmer gleich:
 - a) Mitglieder des Vorstands bei Aktiengesellschaften;
 - b) Geschäftsführer bei Gesellschaften mit beschränkter Haftung;
 - c) Komplementäre bei Kommanditgesellschaften;
 - d) Gesellschafter bei offenen Handelsgesellschaften;
 - e) *Inhaber bei Einzelfirmen*;
 - f) Die nach Gesetz oder Satzung berufenen obersten Vertretungsorgane bei anderen Unternehmensformen
- Die unter a) –f) aufgeführten Personen mitversicherter Unternehmen stehen ebenfalls als Repräsentanten dem VN gleich.

Sachlicher Anwendungsbereich

- Vermögensschaden
- Informationssicherheitsverletzung
- Servicekostenbaustein
- Drittschadenbaustein
- Eigenschadenbaustein

Sachlicher Anwendungsbereich

- A1-1 „Gegenstand der Versicherung“
 - Gegenstand der Versicherung sind Vermögensschäden im Umfang der nachfolgenden Bestimmungen, die durch eine Informationssicherheitsverletzung verursacht worden sind.

Vermögensschäden A1-3 AVB Cyber GDV

Vermögensschäden sind solche Schäden, die weder Personenschäden (Tötung, Verletzung des Körpers oder Schädigung der Gesundheit von Menschen), noch Sachschäden (Beschädigung, Verderben, Vernichtung oder Abhandenkommen von Sachen) sind, noch sich unmittelbar aus solchen Schäden herleiten.

Elektronische Daten sind keine Sachen im Sinne dieser Bedingungen. Der Verlust von elektronischen Daten als Folge des Abhandenkommens von Sachen bleibt als Vermögensschaden versichert.

Informationsfreiheitsverletzung

- A1-2 „Informationssicherheitsverletzung“
 - A1-2.1 Informationssicherheitsverletzung ist eine Beeinträchtigung der Verfügbarkeit, Integrität, oder Vertraulichkeit von elektronischen Daten des Versicherungsnehmers oder von informationsverarbeitenden Systemen, die er zur Ausübung seiner betrieblichen oder beruflichen Tätigkeit nutzt.

Informationssicherheitsverletzung

- A1-2 „Informationssicherheitsverletzung“
 - A1-2.2 Dabei ist es unerheblich, ob sich die elektronischen Daten oder die informationsverarbeitenden Systeme des VN in dessen unmittelbaren Verfügungsbereich befinden oder der VN sich eines externen Dienstleisters bedient.
 - Bedient sich der VN eines externen Dienstleisters, besteht kein Versicherungsschutz für Schäden, die infolge des Ausfalls, der Unterbrechung oder Störung der Dienstleitung entstehen.
 - Beweislast?

Versichertes IT-System

- Bei manchen (wenigen) Versicherern ist die Cloud nicht vom Versicherungsumfang erfasst.
- Behauptung: nahezu jedes Unternehmen nutzt Clouddienste (z.B. MS Office 365)
- Es gibt besonderen Versicherungsschutz für Cloudrisiken (z.B. Cloud-Ausfallversicherung von hendricks)
- ggf. Maklerhaftung prüfen

Informationssicherheitsverletzung

- A1-2.4 Die Informationssicherheitsverletzung muss durch folgende Ereignisse ausgelöst werden:
 - Angriffe von außen auf elektronische Daten oder informationsverarbeitende Systeme des VN
 - Schadprogramme, die auf elektronische Daten oder Informationsverarbeitende Systeme des VN wirken
 - Eine Handlung oder Unterlassung, die zu einer Verletzung von datenschutzrechtlichen Vorschriften durch den VN führt
 - Eingriffe von innen in informationsverarbeitende Systeme des VN
 - Unberechtigte Zugriffe von innen auf elektronische Daten des VN



JOHANNSEN
Rechtsanwälte



Für Drittschäden (Teil C) besteht Versicherungsschutz für Vermögensschäden eines Dritten, aufgrund derer ein Versicherter in Anspruch genommen wird.

Informationssicherheitsverletzung

Eine Informationssicherheitsverletzung im Sinne dieses Vertrags ist eine

- Datenschutzverletzung,
- Datenvertraulichkeitsverletzung,
- Netzwerksicherheitsverletzung.

Datenschutzverletzung

Eine Datenschutzverletzung ist die Verletzung von anwendbaren in- und ausländischen gesetzlichen Regelungen zum Datenschutz (z. B. Bundesdatenschutzgesetz) in Bezug auf elektronische und physische Daten Dritter.

Datenvertraulichkeitsverletzung

Eine Datenvertraulichkeitsverletzung ist eine Verletzung der Vertraulichkeit elektronischer und physischer Daten Dritter,

die sich im Verfügungsbereich der Versicherten befinden und

! die durch Versicherte oder mitversicherte Personen erfolgt.

Netzwerksicherheitsverletzung

Eine Netzwerksicherheitsverletzung ist

07.10.2026
Die Cyberversicherung
Seite 51

51



JOHANNSEN
Rechtsanwälte

ERGO Cyber-Versicherung Kompakt
Versicherungsbedingungen (CVK2019)

Vertragsteil A – Versicherungsschutz für Eigenschäden

A.1 Wiederherstellung von Daten und Programmen

A.1.1 Welche Schäden sind versichert und welche nicht?

A.1.1.1 Der Versicherer leistet Entschädigung für den Fall, dass im versicherten Zeitraum durch

- a) Denial-of-Service Angriffe auf die IT-Systeme des Versicherungsnehmers (DoS Attacke);
- b) zielgerichtete oder nicht zielgerichtete Angriffe durch Dritte oder Mitarbeiter auf IT-Systeme des Versicherungsnehmers;
- c) Diebstahl durch Dritte von stationärer oder mobiler Hardware der IT-Systeme des Versicherungsnehmers oder deren Verlust;
- d) fahrlässige Bedienungsfehler an IT-Systemen des Versicherungsnehmers (z.B. falscher Umgang mit Datenträgern, falsche Befehlseingabe) durch seine Mitarbeiter (als Mitarbeiter gelten auch freie Mitarbeiter, sofern sie in den Betrieb des Versicherungsnehmers eingegliedert sind und der Versicherungsnehmer für sie einzustehen hat.);
- e) unberechtigte Aneignung von Zugangsdaten des Versicherungsnehmers;
- f) eine vollziehbare Verfügung einer Datenschutzbehörde aufgrund einer Datenschutz- oder Datenvertraulichkeitsverletzung beim Versicherungsnehmer

07.10.2026
Die Cyberversicherung
Seite 52

52



JOHANNSEN
Rechtsanwälte



HISCOX
WISSEN VERSICHERT.

Hiscox CyberClear
Bedingungen 10/2020

Versicherungsbedingungen

I. Was ist versichert?

Der Versicherer gewährt den Versicherten im Rahmen der nachstehenden Bedingungen Versicherungsschutz für Vermögensschäden aufgrund folgender Ereignisse (Cyber-Schäden):

- einer Netzwerksicherheitsverletzung;
- eines Bedien- und Programmierfehlers;
- einer Datenrechtsverletzung;
- einer Cyber-Erpressung;
- einer Rechtsverletzung durch Werbung und Marketing.

07.10.2026
Die Cyberversicherung
Seite 53

53



JOHANNSEN
Rechtsanwälte

Bsp: Markel

1. Umfang des Versicherungsschutzes

Der Versicherer gewährt den Versicherten Versicherungsschutz für Cyber- und Dateneigenschäden.

Ein Cyber- und Dateneigenschaden ist die Beschädigung, Zerstörung, Veränderung, Blockierung, Löschung oder der Missbrauch

- der IT-Systeme der Versicherten,

insbesondere der Computer, Server, Netzwerke, Mobiltelefone, Tablets, Telefonanlagen, Videokonferenzsysteme, Datenleitungen sowie Intra- und Extranets,

- der Programme der Versicherten,

insbesondere der Betriebssysteme, Datenbanken, Verwaltungssoftware,

- oder der elektronischen Daten der Versicherten,

insbesondere Auftragsdaten, Kundendaten, Personendaten,

infolge

- eines unbefugten Eingriffs in die IT-Systeme (Hacker-Einbruch, Informationssicherheitsverletzung, Netzwerksicherheitsverletzung),
- eines unbefugten Angriffs mit dem Ziel, die IT-Systeme zu unterbrechen (DoS – Denial of Service),
- einer Infektion eines IT-Systems durch Schadsoftware, insbesondere Viren, Schadcodes und Trojaner,

durch

- Dritte (zum Beispiel Hacker, Kriminelle),
- eine mitversicherte Person bei Gelegenheit einer dienstlichen Tätigkeit mit der Absicht, die Versicherten vorsätzlich zu schädigen (Innentäter).

Für alle Bausteine dieser Cyber-Versicherung gelten sowohl gezielte als auch ungezielte Eingriffe, Angriffe und Infektionen mit Schadsoftware als versichert.

07.10.2026
Die Cyberversicherung
Seite 54

54

Vergleich mit anderen AVB:

- Allianz CyberSchutz 06.2015
 - Der VR bietet Versicherungsschutz für Ansprüche, die gegen Versicherte
 - a. von einem Betroffenen wegen einer Datenschutzverletzung, oder
 - b. von einem Kunden wegen einer Vertraulichkeitsverletzung, oder
 - c. Von einem externen Dienstleister, aufgrund einer Freistellungsverpflichtung für Ansprüche entsprechend Lit a) und b) dieser Ziffer geltend gemacht werden
 - Der Versicherer bietet Versicherungsschutz für Ansprüche, die gegen Versicherte von einem Dritten wegen einer Netzwerksicherheitsverletzung geltend gemacht werden.



Service und Kostenbaustein A2

- A2-1 Forensik/Schadenfeststellungskosten
 - Kosten für Externe Sachverständige zur Ermittlung der Ursache und zur Feststellung des Schadens
 - Sublimit
 - Voraussetzung: vorherige Abstimmung mit VR
- A2-2 Versicherte Kosten im Versicherungsfall
 - Rechtsschutzleistungen
 - Call-Center-Leistungen
- A2-3 Aufwendungen vor Eintritt des Versicherungsfalles
 - Präventionsmaßnahmen

A2-2 Versicherte Kosten im Versicherungsfall

- A2-2.1.a
 - Kosten, die dem VN infolge einer Verletzung von datenschutzrechtlichen Vorschriften zur Prüfung und Erfüllung seiner gesetzlichen und/oder behördlichen Informationspflichten entstehen.
- A2-2.1.b Call-Center-Leistungen
 - muss zusätzlich vereinbart werden
 - Call-Center-Leistungen zur Beantwortung von Anfragen wegen Verletzung von datenschutzrechtlichen Vorschriften
- A2-2.2. Krisenkommunikation und PR-Maßnahmen
 - Maßnahmen zur Erhaltung oder Wiederherstellung der Reputation
 - auch Kosten des PR-Beraters

A2-3 Aufwendungen vor Eintritt des Versicherungsfalls

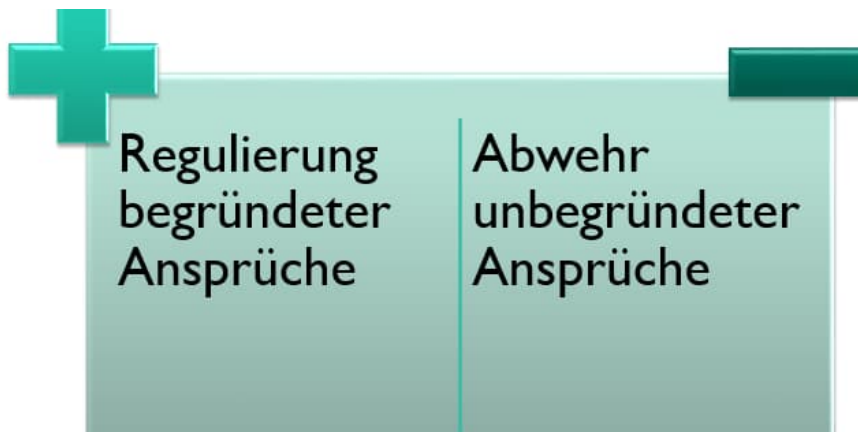
- A2-3.1. Versichert sind Kosten der Schadensvermeidung
 - Voraussetzung unmittelbar bevorstehender Schaden
 - Definition: Ein unmittelbar bevorstehender Schaden liegt vor, wenn aufgrund festgestellter oder objektiver Tatsachen, insbesondere der glaubhaften Androhung oder Kenntnisnahme, von einer Informationssicherheitsverletzung auszugehen ist.
 - Ausschluss: Nicht ersatzfähig sind allgemeine Aufwendungen zur Einhaltung, Nachrüstung, Sicherung oder Sanierung von Informationsverarbeitenden Systemen des VN
 - Voraussetzung: unverzügliche Anzeigepflicht mit Verknüpfung Rechtsfolge B3-4



A3 Drittschadenbaustein

- A3-1 Gegenstand der Versicherung
 - Haftpflicht
 - Abwehr unbegründeter
 - Freistellung von begründeten Ansprüchen Dritter
 - Versicherter Schaden ist Vermögensschaden
 - Erweiterung zu A1-2 Informationssicherheitsverletzung kann auch beim Anspruchsteller eingetreten sein.
- A3-2 Ausschluss Vertragserfüllung
 - wie AHB „Erfüllungsschäden“ etc.
- A3-3 weiterer Ausschluss
 - Vertragliche Vereinbarung oder Zusage verspricht höheren Umfang als ges. Haftpflicht

Leistungsversprechen der Haftpflicht



A3 Drittschadenbaustein

- A3-1 Gegenstand der Versicherung
- Versicherungsschutz besteht im Rahmen des versicherten Risikos für den Fall, dass der Versicherungsnehmer wegen
 - einer Informationssicherheitsverletzung gemäß A1-2,
 - die einen Vermögensschaden zur Folge hat,
 - aufgrund gesetzlicher Haftpflichtbestimmungen privatrechtlichen Inhalts
 - von einem Dritten
 - auf Schadensersatz in Anspruch genommen wird.
 - Dabei kommt es – abweichend von A1-2 – nicht darauf an ob die Informationssicherheitsverletzung beim Versicherungsnehmer, mitversicherten Unternehmen oder beim Anspruchsteller eingetreten ist.

Produktbeispiele

1.1 Versichertes Risiko

Der Versicherer gewährt den Versicherten Versicherungsschutz, wenn sie von einem Dritten aufgrund gesetzlicher – auch verschuldens-unabhängiger – Haftpflichtansprüche privatrechtlichen Inhalts für einen Vermögensschaden (inklusive eines etwaigen immateriellen Schadens) in Anspruch genommen werden, sofern der Schadensersatzanspruch auf einem der nachfolgenden Verstöße 1.3 bis 1.11 beruht.

Die Inanspruchnahme kann unabhängig von einem Cyber- und Dateneigenschaden sein, zum Beispiel auch bei einem Diebstahl oder Verlust von Hardware, Software oder anderen IT-Systemen der Versicherten und/oder einer Veröffentlichung von Daten Dritter durch einen Versicherten.

Produktbeispiele

Teil C Versicherungsschutz für Drittschäden

1 Gegenstand der Versicherung

Versicherungsschutz besteht im Rahmen des versicherten Risikos für den Fall, dass der Versicherungsnehmer wegen einer Informationssicherheitsverletzung gemäß Teil A Ziff. 2, die einen Vermögensschaden zur Folge hat, aufgrund gesetzlicher Haftpflichtbestimmungen privatrechtlichen Inhalts von einem Dritten auf Schadenersatz in Anspruch genommen wird.

Als Vermögensschäden gelten hier auch

- Schäden aus dem Verlust, der Veränderung oder der Blockade elektronischer Daten,
- immaterielle Schäden, die sich aus versicherten Vermögensschäden herleiten. Dazu zählen immaterielle Schäden wegen Persönlichkeitsrechtsverletzungen sowie psychische Beeinträchtigungen.

Produktbeispiele

3. Cyber-Haftpflicht

Der Versicherer gewährt den Versicherten Versicherungsschutz, wenn sie infolge eines versicherten Ereignisses gemäß Ziffern I.1. bis I.4. von einem Dritten aufgrund gesetzlicher Haftpflichtansprüche privatrechtlichen Inhalts für einen Vermögensschaden in Anspruch genommen werden.

Versicherungsschutz in der Cyber-Haftpflicht besteht auch für immaterielle Schäden, die sich aus versicherten Vermögensschäden herleiten. Hierzu zählen immaterielle Schäden aufgrund einer Persönlichkeitsrechtsverletzung sowie psychischer Beeinträchtigungen (mental anguish oder emotional distress).

Darüber hinaus gewährt der Versicherer den Versicherten auch Versicherungsschutz, wenn sie infolge von Werbung und Marketing für das eigene Unternehmen gemäß Ziffer I.5. von einem Dritten aufgrund gesetzlicher Haftpflichtansprüche privatrechtlichen Inhalts für einen Vermögensschaden in Anspruch genommen werden (Werbe-Haftpflicht).

Produktbeispiele

3. Drittschadenversicherung

3.1. Gegenstand der Versicherung:

Der **Versicherer** gewährt Versicherungsschutz für den Fall, dass die **Versicherten** erstmals während der **Versicherungsperiode** oder einer ggf. vereinbarten Nachmeldefrist von einem **Dritten** in Anspruch genommen werden aufgrund gesetzlicher Haftpflichtbestimmungen privatrechtlichen Inhalts auf Ersatz eines **Vermögensschadens** aufgrund

- eines Cyber-Vorfalles (1.2),
- einer Datenschutz- und Datenvertraulichkeitsverletzung (1.5).

In Erweiterung hierzu besteht im Rahmen der Drittschadenversicherung auch Versicherungsschutz für immaterielle Schäden natürlicher Personen, aufgrund einer Persönlichkeitsrechtsverletzung im Zusammenhang mit Datenschutz und Datenvertraulichkeitsverletzung (1.5)

Haftpflichtbestimmungen privatrechtlichen Inhalts

- § 280 BGB
- § 823 Abs. 1 BGB
 - Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb
- § 823 Abs. 2 BGB i.V.m.
 - § 202 StGB (Ausspähen von Daten)
 - § 202b StGB (Abfangen von Daten)
 - § 263a StGB (Computerbetrug)
 - § 303a StGB (Datenveränderung)
 - § 303b StGB (Computersabotage)
 - § 23 GeschGeh (Verrat von Geschäfts- und Betriebsgeheimnissen) [entspricht §17 UWG a.F.]
- Art. 82 DS-GVO

Exkurs: Art. 82 DS-GVO

- Abs. 1: Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.
- Abs. 2: Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde.
- Anspruch ist Verschuldensunabhängig!
- Ersatz von Schäden wegen Verletzung von Persönlichkeitsrechten ist aber nach A1-17.2 AVB Cyber (GDV 2017) bzw. A1-17.11 AVB Cyber GDV 2024 grds. ausgeschlossen, aber optional versicherbar!

Inanspruchnahme des VN durch einen Dritten

- Versicherungsschutz besteht nur (bzw. erst dann) wenn der VN von einem Dritten in Anspruch genommen wird
- Dritter ist, wer einen Schadensersatzanspruch als Rechteinhaber geltend macht.
 - Kann auch grds. mitversicherte Person sein
 - aber Ausschluss in A3-7.2 AVB Cyber (GDV)

A3 Drittschadenbaustein

- A3-4 Erweiterte Deckungsbausteine
 - A3-4.1 Rechtswidrige elektronische Kommunikation
 - Persönlichkeitsrechts-, Namensrechts, Urheber- oder Wettbewerbsrechtsverletzungen
 - Sublimit
 - A3-4.2 E-Payment
 - Vertragsstrafen im Zusammenhang E-Payment Service Provider wegen einer Verletzung eines Payment Card Industrie (PCI) Datensicherheitsstandards (Bsp. Kreditkarte)
 - Erweiterung zu A1-2 Informationssicherheitsverletzung kann auch beim Anspruchsteller eingetreten sein.
 - A3-4.3 Vertragliche Schadensersatzansprüche
 - grds. ausgeschlossene vertragliche Ansprüche können wiedereingeschlossen werden.

A3 Drittschadenbaustein

A3-4 Erweiterte Deckungsbausteine

A3.4.1 Verletzung von Datenschutzgesetzen

Mitversichert ist teilweise abweichend von A1-17.11 auch die gesetzliche Haftpflicht des Versicherungsnehmers wegen Schäden aus der Verletzung von Datenschutzgesetzen durch Verarbeitung personenbezogener Daten.

Verarbeitung ist jeder, mit oder ohne Hilfe automatisierter Verfahren, ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Mitversichert sind gesetzliche Haftpflichtansprüche wegen Schäden von Versicherten (Versicherungsnehmer oder mitversicherte Personen) untereinander. Der Ausschluss in A3-7.2 findet insoweit keine Anwendung.

A3 Drittschadenbaustein

■ A3-7 Besondere Ausschlüsse

- Rückruf
- Ansprüche der versicherten untereinander
- Ansprüche verbundener Unternehmen
- Angehörigenklausel



A4 Eigenschadenbaustein

■ A4-1 Betriebsunterbrechung/Ertragsausfall

- Bei einer ISV besteht V-Schutz für eine Betriebsunterbrechung
- BU liegt vor, wenn infolge der ISV elektronische Daten oder informationsverarbeitende Systeme des VN nicht zur Verfügung stehen oder nicht die übliche Leistung erbringen und daraus ein Schaden entsteht.
- Unterbrechungsschaden sind Betriebsgewinn und die fortlaufenden Kosten
- Begrenzung auf Haftzeit (Neubeginn der Haftzeit)

A4 Eigenschadenbaustein

■ A4-1.2 Besondere Ausschlüsse

- Zeitraum geplante Abschaltung informationsverarbeitende Systeme
- Geplante Löschung oder Veränderung elektronische Daten
- Durch Einführung neuer informationsverarbeitende Systeme oder Verfahren sowie Software (relevante Sicherungsupdates ausgenommen)
- Durch Einsatz ungetesteter Systeme oder Verfahren
- Durch Verwendung von Systemen, Verfahren sowie Software ohne Berechtigung des VN

A4 Eigenschadenbaustein

■ A4-1.3 Umfang der Entschädigung

- Höhe des vereinbarten Tagessatzes für Dauer der BU
- Aber keine Entschädigung bei längerer Dauer durch
 - außergewöhnliche, während der Unterbrechung hinzutretender Ereignisse, mit deren Eintritt als Folge der ISV nicht gerechnet werden muss.
 - behördliche Wiederherstellungs- oder Betriebsbeschränkungen
 - fehlende finanzielle Mittel
 - vorgenommene Veränderungen oder Verbesserungen
 - Sach- oder Personenschäden

Beispiele aus der Praxis

2. Leistungen des Versicherers

Der Versicherer ersetzt den Versicherten den Ertragsausfall für den Zeitraum der versicherten Betriebsunterbrechung oder -beeinträchtigung, soweit die Versicherten die fortlaufenden Kosten und den Betriebsgewinn infolge und während der Unterbrechung oder Beeinträchtigung nicht erwirtschaften können.

Der Ertrag setzt sich zusammen aus den fortlaufenden Kosten und dem Betriebsgewinn der Versicherten.

Bei der Berechnung des Ertragsausfalls sind alle Umstände zu berücksichtigen, die das Geschäftsergebnis der Versicherten ohne Eintritt der Betriebsunterbrechung oder -beeinträchtigung günstig oder ungünstig beeinflusst hätten.

Der Versicherer ersetzt zudem Aufwendungen, die im Betrieb der Versicherten normalerweise nicht entstehen und nur infolge der Betriebsunterbrechung oder -beeinträchtigung zur Fortführung des Betriebs aufgewendet werden müssen (Mehrkosten).

2.4.4 Ertragsausfall



Ertragsausfall ist der Betriebsgewinn und die fortlaufenden Kosten, die nach einem entschädigungspflichtigen Schaden durch die Versicherten nicht erwirtschaftet werden können (Unterbrechungsschaden).

A4 Eigenschadenbaustein

- A4-1.3.2 Entschädigungsgrenze
 - Beschränkt auf V-Summe je Versicherungsfall
 - Beschränkt auf Jahresversicherungssumme
- A4-1.3.3 Zeitliche Selbstbeteiligung
 - Kann vereinbart werden
 - Aber Achtung BU in der Regel eher kurz!

A4 Eigenschadenbaustein

- A4-2 Wiederherstellung von Daten
 - Bei ISV besteht V-Schutz für notwendige Aufwendungen zur Wiederherstellung der von der ISV betroffenen Daten sowie Entfernung der Schadsoftware
 - Versicherte Daten, sind alle solche die der VN nutzen darf und sich auf System von VN oder mitversichertem Unternehmen befinden.
- A4-2.3 Besondere Ausschlüsse
 - wie A4-1.2
- A4-2.4.1 Versicherungssumme und Jahreshöchstentschädigung
 - wie A4-1.3.2

A4 Eigenschadenbaustein

- A4-2.4.2 Umfang der Entschädigung
 - Entschädigung in Höhe der notwendigen Aufwendungen zur Wiederherstellung der von der ISV betroffenen Daten in den Zustand vor der ISV sowie für die Entfernung der Schadsoftware
 - Keine Entschädigung für:
 - Mehrkosten durch Änderungen oder Verbesserungen, die über die Wiederherstellung hinausgehen
 - Kosten für die Wiederherstellung von Daten nach Ablauf von ...Zeitraumen... nach Beeinträchtigung der Daten durch die ISV



Auslegung und Beweislast von Ausschlüssen in AVB

- Dabei ist zu berücksichtigen, dass das Versicherteninteresse bei Risiko- und Leistungsausschlussklauseln in der Regel dahin geht, dass der Versicherungsschutz nicht weiter verkürzt wird, als der erkennbare Zweck einer Klausel dies gebietet. Der durchschnittliche VN braucht nicht mit Lücken im Versicherungsschutz zu rechnen, ohne dass die Klausel ihm dies hinreichend verdeutlicht. Deshalb sind Risikoausschlussklauseln nach ständiger Rechtsprechung des Senats eng und nicht weiter auszulegen, als es ihr Sinn unter Beachtung ihres wirtschaftlichen Zwecks und der gewählten Ausdrucksweise erfordert. (st.Rspr. BGH z.B. VersR 2020, 283)
- VR trägt Darlegungs- und Beweislast

Allgemeine Ausschlüsse A1-17

- Auch über die Kriegsklausel wird gestritten (Mondelez / Zurich)



The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy steps:

1. Download the Tor Browser at "<https://www.torproject.org/>". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:
<http://petya37huyoki.onion/BdtSQe>
<http://petya5koahstf7sv.onion/BdtSQe>
3. Enter your personal decryption code there:
 3bP8up-Rd321r-xrDBS3-XGA1F9-R2THSB-Xyahmh-b3HWE9-WeYMI1-BemRfv-v1RX5A-BtDLTG-QfbbBF-uehezH-U7b5T7-ucJuHb

If you already purchased your key, please enter it below.

Key: xxC9ChuLWuJpL19
 Decrypting sector 25178 of 39136 (64%)

Allgemeine Ausschlüsse A1-17

- A1-17.1 Vorvertraglichen Informationssicherheitsverletzungen
 - Alle Schäden vor Beginn des Vertrages (formeller Beginn)
- A1-17.2 bis 17.4, 17.13 Übliche Kumul-Ausschlüsse Krieg, Politische Gefahren, Terror, Kernenergie
- A1-17.5 Besonderer Kumul-Ausschluss: Ausfall der Infrastruktur
 - Ein Ausfall der Infrastruktur liegt vor, wenn
 - Gebietskörperschaften oder wesentliche Teile hiervon, wie Stadtteile, Gemeinden, Städte oder Kreise oder
 - Netzstrukturen, die der überregionalen Informationsvermittlung, insbesondere Telefon-, Internet- oder Funknetze dienen, oder
 - besondere Einrichtungen der Daseinsvorsorge
 - oder sonstige Infrastrukturbetriebe vom Ausfall betroffen sind.

Allgemeine Ausschlüsse A1-17

- A1-17.5 Besonderer Kumul-Ausschluss: Ausfall der Infrastruktur
- Ein Ausfall der Infrastruktur liegt vor, wenn
 - Gebietskörperschaften oder wesentliche Teile hiervon, wie Stadtteile, Gemeinden, Städte oder Kreise oder
 - Netzstrukturen, die der überregionalen Informationsvermittlung, insbesondere Telefon-, Internet- oder Funknetze dienen, oder
 - besondere Einrichtungen der Daseinsvorsorge
 - oder sonstige Infrastrukturbetriebe vom Ausfall betroffen sind.

Allgemeine Ausschlüsse A1-17

- A1-17.6 Fahrzeuge
 - Versicherungsfälle oder Schäden im Zusammenhang mit Kraftfahrzeugen
- A1-17.7 Löse-/Erpressungsgeld
- A1-17.8 Finanzmarkttransaktionen
- A1-17.9 Abfluss von Vermögenswerten
- A1-17.10 Vorsatz und wissentliche Pflichtverletzungen
- A1-17.11 Behördliche Maßnahmen, Strafen/Bußgelder
- A1-17.12 Verletzung von Immaterialgüterrechten.

Ausschluss A1-17.7

- A1-17.7 Löse-/Erpressungsgeld
 - Versicherungsfälle oder Schäden aus der Zahlung von Löse-/Erpressungsgeldern oder Erfüllung von Erpressungsforderungen.
 - Insbes. bei Ransomware-Angriff
 - Grund (bisher) Verbot durch Bafin Rundschreiben 3/98
 - Verbot Erpressungsgelder bei Bündelpolicen zu versichern
 - Aber Bafin hat Verbot im September 2017 aufgehoben!
- Folge Versicherer dürfen Erpressungsgelder in Cyber-Police versichern
 - Es gibt aber Einschränkungen (Werbeverbot)

Am Markt vorhandene Klauseln

2.9. Lösegeld

Der Versicherer ersetzt das gezahlte Lösegeld bzw. bei Bezahlung eines Lösegeldes in Form von Kryptowährungen, Waren oder Dienstleistungen deren Marktwert zum Zeitpunkt der Beschaffung.

Problematik Lösegeldzahlungen

- Wirksamkeit der Klausel A1-17.7?
 - ggf. Verstoß gegen § 87 VVG (halbzwingend – außer bei Großrisiko § 210 VVG)
(a.A. Langheid/Wandt/Rudkowski, 3. Aufl. 2025, Kap. 37. Rn. 260)
- Strafbarkeitsrisiken für Unternehmens- IT-Verantwortliche? (vgl. Ballo/Pieper/Schneider, r+s 2023, 741)
 - mögl. wg. Unterstützung krimineller Vereinigungen, §§129 Abs. 1 S. 2 Alt.1, 129b Abs. 1 S. 1,2 StGB;
 - Terrorismusfinanzierung, § 89c Abs. 1 StGB;
 - Untreue, § 266 Abs. 1 StGB;
 - Geldwäsche, § 261 StGB
 - Rechtfertigender Notstand, § 34 StGB?

Ausschluss A1-17.8

- A1-17.8 Finanzmarkttransaktionen
 - Versicherungsfälle oder Schäden aufgrund oder im Zusammenhang mit jedweder Form des Kaufs oder Verkaufs von Wertpapieren, Rohstoffen, Derivaten, Devisen, Anleihen und vergleichbaren Wertanlagen

Ausschluss A1-17.9

- A1-17.9 Abfluss von Vermögenswerten
 - Versicherungsfälle oder Schäden aus dem Abfluss von Vermögenswerten der Versicherten, die im Zusammenhang mit einer Informationssicherheitsverletzung entstehen.

Die Masche mit dem falschen Chef

Unternehmen werden immer häufiger Opfer des sogenannten „CEO-Fraud“ oder auch „Fake-President-Fraud“. Die Grundidee gleicht dem bekannten „Enkeltrick“. Durch immer weitergehende Professionalisierung der Täter wird es jedoch trotz der medialen Aufmerksamkeit schwerer, sich zu schützen.

- CEO-Fraud-Fälle sind nach den AVB Cyber (GDV) nicht versichert

Am Markt vorhandene Klauseln

2.8. Cyber-Betrug (sofern im Versicherungsschein besonders vereinbart)

Bei Cyber-Betrugsfällen in Form von Fake-President- bzw. CEO-Fraud- und Lieferantenbetrugs-Fällen ersetzt der Versicherer Vermögensschäden, die einem Versicherten dadurch entstehen, dass unmittelbar infolge einer Netzwerksicherheitsverletzung gemäß Ziffer I.1. einem Dritten eine Täuschung einer mitversicherten natürlichen Person (nicht jedoch eines Repräsentanten) möglich wird, die zu einem Abfluss von Geldern, Waren oder Wertpapieren führt.

Die Obliegenheiten nach Eintritt des Versicherungsfalles gemäß Ziffer IV.15.1. werden um die folgende Anzeige bestimmter Umstände ergänzt:

- im Falle von Cyber-Betrug
 - alle angemessenen Schritte zu unternehmen, um abhandengekommene Gelder, Waren oder Wertpapiere zurückzuerlangen oder einzufrieren;
 - unverzüglich Strafanzeige zu erstatten.

Für Cyber-Betrug gilt die im Versicherungsschein benannte Entschädigungsgrenze.

LG Hagen, Urt. v. 15.10.2024, r+s 2025, 28 mit Anm. v. Schilbach

Cyber-Versicherung, Begriff der Netzwerksicherheitsverletzung

BGB § 307 Abs. 1 Satz 2 und Abs. 3 Satz 1; AVB für die Versicherung von Cyber-Risiken, Stand: April 2019 Teil A Ziff. 3 und 4, Teil D Ziff. 1

1. Der durchschnittliche VN versteht den Begriff der Netzwerksicherheitsverletzung dahingehend, dass es zu einer Verletzung der Sicherheit des eigenen Netzwerks gekommen sein muss und es nicht ausreicht, dass das Netzwerk eines Dritten betroffen ist.
2. Der bloße Empfang einer betrügerischen (Phishing-)E-Mail begründet noch keine Netzwerksicherheitsverletzung.
3. Für eine Cyber-Versicherung ist typisch und für den durchschnittlichen VN erkennbar, dass nur das Risiko der eigenen IT-Systeme geschützt werden soll und Hacker-Angriffe, die lediglich in mittelbarer Weise Auswirkungen für den VN haben können, nicht vom Versicherungsschutz umfasst sind.

Vorsatz und wissentliche Pflichtverletzung

A1-17.10 Vorsatz und wissentliche Pflichtverletzung

Versicherungsansprüche aller Personen, die den Schaden vorsätzlich oder durch wissentliches Abweichen von Gesetz, Vorschrift, Beschluss, Vollmacht oder Weisung oder durch sonstige wissentliche Pflichtverletzungen herbeigeführt haben.

- § 81 VVG (für Assistance und Eigenschadenbaustein einschlägig) wird dadurch abbedungen (a.A. *Höld* VersR 2023, 353).

A1-17.9 Vorsatz und wissentliche Pflichtverletzung

Versicherungsansprüche aller Personen, die den Schaden vorsätzlich oder durch wissentliches Abweichen von Gesetz, Vorschrift, Beschluss, Vollmacht oder Weisung oder durch sonstige wissentliche Pflichtverletzungen herbeigeführt haben.

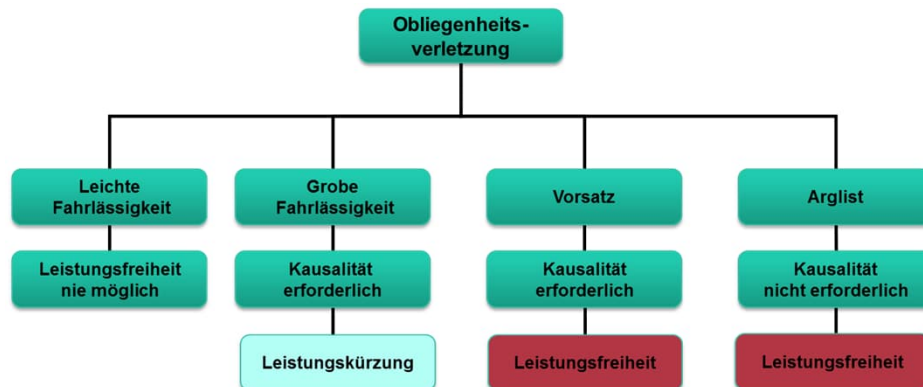
§ 81 Abs. 2 VVG findet keine Anwendung.



Vorvertragliche Anzeigepflichtverletzung

- Eine vorvertragliche Anzeigepflicht liegt vor, wenn der VN Fragen in Textform, welche sich auf einen Gefahrerheblichen Umstand bezieht, objektiv falsch beantwortet. Relevant sind in der Cyberversicherung insbes. Fragen zur Zugangssicherung und zu Sicherheitsupdates.
- z.B. LG Tübingen, NJW-RR 2023, 1194
 - Es kann dahin stehen, ob die KI. die ihr gestellten Risikofragen vorsätzlich oder grob fahrlässig falsch beantwortet und insofern ihre vorvertragliche Anzeigepflicht nach B3-1.1 AVB verletzt hat. Jedenfalls hat die KI. gem. § 21 Abs. 2 S. 1 VVG nachgewiesen, dass eine möglicherweise falsche Beantwortung der Risikofragen weder für den Eintritt des Versicherungsfalls noch für die Feststellung oder den Umfang der Leistung ursächlich gewesen ist (Kausalitätsgegenbeweis).

Regime der Obliegenheitsverletzungen



Obliegenheiten vor Eintritt des Versicherungsfalls A1-16

- Üblicher Aufbau:
 - In A1-16.1 bis 16.2 werden Obliegenheiten aufgezählt
 - In A1-16.3 Verknüpfung mit Rechtsfolgen (B3-4)
 - Verweis auf Obliegenheiten bei und nach Eintritt des Versicherungsfalls
- A1-16.1 bis 16.2 Obliegenheiten:
 - Unterscheidung Nutzer und Befugnisebenen (Admin)
 - Schutz gegen unberechtigten Zugriff (Firewall, 2-Faktor-Authentifizierung)
 - Üblicher Schutz gegen Schadsoftware mit automatischen Updates (Virens Scanner, Code signing, Application Firewall o.Ä.)
 - Patch-Management-Verfahren
 - Wöchentlicher Sicherungsprozess (getrennte Aufbewahrung der Sicherungskopie)

Stand der Technik-Klauseln

- Es gibt Klauseln, wie z.B. die Verpflichtung des VN angemessene, dem Stand der Technik entsprechende technische Einrichtungen und Verfahren zur Informationssicherheit zu unterhalten.
- unstritten

Obliegenheiten vor Eintritt des Versicherungsfalls

- A1-16.2 Darüber hinaus hat der VN
 - Alle gesetzlichen, behördlichen sowie vertraglich vereinbarten Sicherheitsvorschriften einzuhalten.
- Klausel ist wirksam vgl. BGH Urt. v. 25.09.2024 - IV ZR 350/22
- In Betracht kommen Regelungen aus:
 - DSGVO
 - BDSG
 - TKG
 - BSIG nebst Rechtsverordnungen

Gefahrerhöhung

- Die Gefahrerhöhung und deren Rechtsfolgen wird in B3-2.AVB Cyber geregelt und entspricht den gesetzlichen Regelung der §§ 23 ff.VVG.
- z.B. LG Tübingen, NJW-RR 2023, 1194:
 - Es kann offen bleiben, ob nach Vertragsschluss eine Gefahrerhöhung eingetreten ist, indem die Kl. weitere Software-Updates nicht durchgeführt bzw. anders als in der Veranstaltung am 13.2.2020 angekündigt die veralteten Server (noch) nicht ausgetauscht hat. Da der Kl. der Kausalitätsgegenbeweis gelingt (s. oben), wäre die Bekl. selbst bei einer solchen Gefahrerhöhung nicht leistungsfrei; auch eine Kürzung des Anspruchs ist ausgeschlossen (Rn. 61).

Grob-fahrlässige Herbeiführung des Versicherungsfalls

- § 81 Abs. 2 VVG ist oftmals abbedungen.
- z.B. LG Tübingen, NJW-RR 2023, 1194

Der Anwendungsbereich des § 81 Abs. 2 VVG ist dann nicht eröffnet, wenn die betreffende Gefahrenlage bereits bei Vertragsschluss bestand und bereits Grundlage der Risikoprüfung des VR war bzw. hätte sein. So liegt der Fall hier. Bei der Kl. hat sich die Risikolage bis zum 29./30.5.2020 gegenüber dem Zustand bei Vertragsschluss im April 2020 nicht geändert. Denn bereits damals verfügte die Kl. weder über eine Zwei-Faktoren-Authentifizierung noch über ein Monitoring oder eine andere vergleichbare Maßnahme zur Vermeidung von Cyber-Angriffen. Die Bekl. hätte es selbst in der Hand gehabt, die Existenz solcher zusätzlichen Sicherheitsmaßnahmen durch passende Risikofragen abzuklären.

Unterversicherung § 75 VVG

- Ist die Versicherungssumme erheblich niedriger als der Versicherungswert zur Zeit des Eintrittes des Versicherungsfalles, ist der Versicherer nur verpflichtet, die Leistung nach dem Verhältnis der Versicherungssumme zu diesem Wert zu erbringen.

OLG Schleswig, Beschl.V. 09.01.2025, 16 U 63/24 zur Anfechtung

- Sachverhalt: Der IT-Leiter der VN hat Risikofragen bei Antragstellung beantwortet, ohne genaue Kenntnisse über die erfragten Umstände gehabt zu haben, um die Fragen valide beantworten zu können. (Antworten ins Blaue hinein).
- Entscheidung: Der Senat hat die Berufung der Klägerin zurückgewiesen. Die Risikofragen seien ausgehend vom Verständnishorizont eines durchschnittlichen Versicherungsnehmers vor dem Hintergrund der Versicherung, die abgeschlossen werden soll, auszulegen. Hier gehe es um eine Cyber-Versicherung für ein Unternehmen mit mehr als 400 Mitarbeitern und einem Jahresumsatz von rund 143,5 Millionen Euro, das umfassend im Online-Geschäft tätig ist. Dementsprechend könne der Versicherer bei der Beantwortung der Fragen eine gewisse Sorgfalt erwarten, die sämtlich erkennbar vereinzelt auf spezifische technische Sachverhalte zielen.



Silent Cyber

- Haftpflichtversicherung
- Berufshaftpflichtversicherung für Rechtsanwälte
- Sachversicherung
- Technische Versicherung
- Vertrauensschadenversicherung
- D&O Versicherung
- Verhältnis zur Cyberversicherung
 - Neben- und Mehrfachversicherung
 - Subsidiaritätsklauseln

Silent Cyber

- Ob in herkömmlichen Versicherungsprodukten Cyber-Risiken schlummern hängt insbes. davon ab, ob elektronische Daten dem Sachschadenbegriff unterfallen oder nicht.
- Sachschadenbegriff ist nach der Rspr. des BGH differenziert zu betrachten und abhängig vom einschlägigen Versicherungszweig, vgl. BGH, r+s 2010, 376 ff.; *Bertsch*, Silent Cyber, S.36.

Silent Cyber in der Haftpflichtversicherung?

- V-Schutz nach AHB erstreckt sich nach Ziffer 1.1 AHB auf Personen- Sach- und daraus resultierende Vermögensschäden (unechte Vermögensschäden)
- Kommt es in den AHB darauf an, ob elektronische Daten unter den Sachschadensbegriff fallen?
- Nein!

Ausschlüsse in den AHB

- 7.15 Haftpflichtansprüche wegen Schäden aus dem Austausch, der Übermittlung und der Bereitstellung elektronischer Daten, soweit es sich handelt um Schäden aus
- (1) Löschung, Unterdrückung, Unbrauchbarmachung oder Veränderung von Daten,
 - (2) Nichterfassen oder fehlerhaftem Speichern von Daten,
 - (3) Störung des Zugangs zum elektronischen Datenaustausch,
 - (4) Übermittlung vertraulicher Daten oder Informationen.
- 7.16 Haftpflichtansprüche wegen Schäden aus Persönlichkeits- oder Namensrechtsverletzungen.

Gleiches gilt grds. für die AVB BHV (GDV Stand 09.2021)

A1-6.12 Vermögensschäden

A1-6.12.1 Versichert ist die gesetzliche Haftpflicht des Versicherungsnehmers wegen Vermögensschäden, die weder durch Personen- noch durch Sachschäden entstanden sind.

Vom Versicherungsschutz ausgeschlossen sind Ansprüche wegen Vermögensschäden

- h) aus
 - Rationalisierung und Automatisierung,
 - Datenerfassung, -speicherung, -sicherung, -wiederherstellung,
 - Austausch, Übermittlung, Bereitstellung elektronischer Daten.
- i) aus der Verletzung von Persönlichkeitsrechten und Namensrechten, gewerblichen Schutzrechten und Urheberrechten sowie des Kartell- oder Wettbewerbsrechts;

Wiedereinschluss (AVB BHV)

A1-6.13.1 Verletzung von Datenschutzgesetzen

Versichert ist die gesetzliche Haftpflicht des Versicherungsnehmers wegen Schäden – auch Vermögensschäden, die weder durch Personen- noch durch Sachschäden entstanden sind, sowie immaterielle Schäden – aus der Verletzung von Datenschutzgesetzen durch Verarbeitung personenbezogener Daten.

Verarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Versichert sind gesetzliche Haftpflichtansprüche wegen Vermögensschäden, die weder durch Personen- noch durch Sachschäden entstanden sind, sowie wegen immaterieller Schäden von Versicherten (Versicherungsnehmer oder mitversicherte Personen) untereinander. Der Ausschluss in A1-7.3 findet insoweit keine Anwendung.

Die Ausschlüsse in A1-6.12.1, A1-7.9 und A1-7.26 finden keine Anwendung.

Wiedereinschluss 2 (AVB BHV)

A1-6.13.2 Übertragung elektronischer Daten

A1-6.13.2.1 Versichert ist die gesetzliche Haftpflicht des Versicherungsnehmers wegen Schäden – auch Tätigkeitsschäden und Vermögensschäden, die weder durch Personen- noch durch Sachschäden entstanden sind – aus dem Austausch, der Übermittlung und der Bereitstellung elektronischer Daten (z. B. im Internet, per E-Mail oder mittels Datenträger) ausschließlich aus

- a) der Löschung, Unterdrückung, Unbrauchbarmachung oder Veränderung von Daten (Datenveränderung) bei Dritten durch Computer-Viren und/oder andere Schadprogramme;
- b) der Datenveränderung aus sonstigen Gründen sowie der Nichterfassung und fehlerhaften Speicherung von Daten bei Dritten und zwar wegen
 - sich daraus ergebender Personen- und Sachschäden, nicht jedoch weiterer Datenveränderungen sowie
 - der Kosten zur Wiederherstellung der veränderten Daten bzw. Erfassung/korrekten Speicherung nicht oder fehlerhaft erfasster Daten;
- c) der Störung des Zugangs Dritter zum elektronischen Datenaustausch.

AVB BHV

- Ergebnis:
 - In den AVB BHV sind Silent Cyber- Risiken teilw. gedeckt.
 - Folgeschäden die durch eine Datenveränderung verursachten Betriebsunterbrechungsschaden beim Dritten sind versichert
 - und zwar bis zur V-Summe

Silent Cyber in der Haftpflichtversicherung? (Quelle: Golem)

SERVERKONFIGURATION GELÖSCHT

Katze verursacht vierstündigen Systemausfall

In den USA hat eine Katze einen vierstündigen Systemausfall ausgelöst, indem sie auf die Tastatur eines Technikers sprang.



6. Oktober 2023, 12:30 Uhr, Marc Stöckel

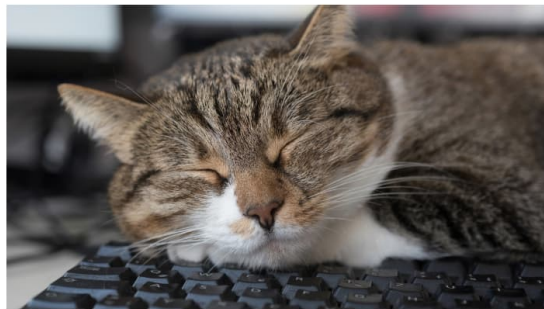


Bild: pixabay.com / hugobn

07.10.2026

Die Cyberversicherung

Seite 15

115

Berufshaftpflichtversicherung für Rechtsanwälte

- § 1 AVB-RSW
- Gegenstand des Versicherungsschutzes
 - Der Versicherer bietet dem Versicherungsnehmer Versicherungsschutz für den Fall, dass er wegen eines bei der Ausübung beruflicher Tätigkeit von ihm selbst oder einer Person, für die er nach § 278 oder § 831 BGB einzustehen hat, begangenen Verstoßes von einem anderen auf Grund gesetzlicher Haftpflichtbestimmungen privatrechtlichen Inhalts für einen Vermögensschaden verantwortlich gemacht wird.

07.10.2026

Die Cyberversicherung

Seite 16

116

Berufshaftpflichtversicherung für Rechtsanwälte

- Ausschlüsse in § 4 AVB-RSV
 - Kein Ausschluss entsprechend Ziffer 7.15 u 7.16 AVB
 - Wissentliche Pflichtverletzung kann relevant sein.
- Silent Cyber-Risiken sind versichert, soweit diese berufsbezogen sind.
 - Bsp: ReFa leitet eine Mail mit einer Datei an einen Mandanten weiter, welche ein Schadprogramm enthält.

117

Sachversicherung

- Bei den „Versicherten Gefahren“ z.B. § 1 Nr. 1 AFB 2010 sind Cyber-Risiken nicht enthalten.
 - Es muss also gebrannt haben!
- § 3 Nr. 1 S. 3 AFB 2010 Verlust, Veränderung und Nichtverfügbarkeit von Daten- und Programmen ist nur versichert, wenn ein versicherter Schaden an einem Datenträger eingetreten ist.
- Es ist denkbar, dass ein Netzwerk durch einen Angriff dergestalt überlastet wird, dass etwas brennt oder explodiert.

118

Sachversicherung

- Gleiches gilt grds. für die Betriebsunterbrechungsversicherung (z.B. FBUB)
- Manche VR gehen teilweise dazu über, im Rahmen der Betriebsunterbrechungsversicherung auf das Sachschadenerfordernis vollständig zu verzichten. Die damit sowieso schon bestehende Gefahr von Kumulrisiken aufgrund von weltweiten Abhängigkeiten, wird durch die nunmehr vollständig mitversicherten Cyber-Risiken noch erheblich verstärkt.
- Einschluss Rückwirkungsschäden
 - (Sach-)Schaden entsteht bei Zulieferer oder Abnehmer

Technische Versicherung

- Maschinenversicherung
- Teil A § 2 AMB 2011:
- Der Versicherer leistet Entschädigung für
 - unvorhergesehen
 - eintretende
 - Beschädigungen oder Zerstörungen
 - von versicherten Sachen.
- Insbesondere wird Entschädigung geleistet für Sachschäden
 - a) Bedienungsfehler, Ungeschicklichkeit oder Vorsatz Dritter
 - d) Versagen von Mess-, Regel- oder Sicherheitseinrichtungen;

Technische Versicherung

- Maschinenversicherung
- Sachschadenbegriff der AMB 2011
 - Ein Sachschaden ist anzunehmen, wenn die Brauchbarkeit oder der Wert der Sache durch eine von außen (insoweit a. A. B/M/v. Rintelen A. § 2 AMB Rn. 17) kommende Einwirkung auf die Sachsubstanz beeinträchtigt wird.
 - Dazu ist eine Verletzung der Sachsubstanz nicht erforderlich, eine Einwirkung reicht aus (BGH VersR 1979, 853, 854).
 - Eine Substanzbeeinträchtigung ohne Bedeutung für die Funktion reicht nicht aus (BGH VersR 1979, 853, 855).
- Versicherte Sachen
 - Teil A § 1 AMB 2011 „stationären Maschinen, maschinellen Einrichtungen und sonstige technische Anlagen, sobald sie betriebsfertig sind.“
 - von dieser Definition sind „Daten“ nicht erfasst.

Technische Versicherung

- Elektronikversicherung
- Daten sind von den Versicherten Sachen nach § 1 ABE nicht erfasst
- Deckungserweiterung TK 1911 (Datenversicherung) und TK 1928 (Software-Versicherung)
- Nach Ziffer 3 TK 1911 leistet der VR allerdings nur Entschädigung für den Fall, dass der Verlust, die Veränderung oder Nichtverfügbarkeit der Daten oder Programme infolge Über- oder Unterspannung durch Blitz oder infolge eines dem Grunde nach versicherten (Sach-)Schadens gemäß § 2 ABE 2011 am Datenträger oder der Datenverarbeitungsanlage eingetreten ist. Dadurch erfasst der Versicherungsschutz weiterhin keine reinen Datenbeeinträchtigungen durch Schadprogramme.

Technische Versicherung

- Elektronikversicherung
- Durch Vereinbarung der Klausel TK 1928 (Software-Versicherung) erweitert sich der Versicherungsschutz im Bereich der Daten- und Programmschäden um weitere benannte Gefahren.
- Nach Ziffer 3 b) cc) TK 1928 sind vorsätzliche Programm- oder Datenveränderungen durch Dritte in schädigender Absicht versichert.
- Wiederausschluss: Ziffer 3 c TK 1928: kein V-Schutz wegen Schäden durch Daten und Programme mit Schadfunktion, Programmfehlern oder DDoS-Angriffe.
- Versichert sind nur solche Silent-Cyber-Risiken in denen sich ein Hacker ohne den Einsatz von Schadprogrammen Zugang zu den IT-Systemen verschafft und dort Daten beeinträchtigt.
 - z.B. durch „Erschleichen“ Hallo ich bin der Nick von der IT und bräuchte ihr...

Technische Versicherung

- Elektronikversicherung
- Nach der Klausel TK 1929 ABE (20) „Erweiterte Datenversicherung“ können nunmehr auch vorsätzliche Angriffe Dritter versichert werden. Nach dem Klauselwortlaut fallen darunter ausdrücklich auch DDoS-Angriffe oder Angriffe mittels Schadsoftware.

Vertrauensschadenversicherung

Eingriffe Dritter in das EDV-System

§ 15 Für welche unmittelbaren Schäden, verursacht durch Eingriffe Dritter in das EDV-System (Hackerschäden), besteht Versicherungsschutz?

Versicherungsschutz besteht für unmittelbare Schäden, die einem versicherten Unternehmen durch vorsätzliche, rechtswidrige und zielgerichtete Eingriffe Dritter in das EDV-System des versicherten Unternehmens (Hackerschäden) zugefügt werden, soweit sich ein Dritter in Höhe des Schadens bereichert hat und ein Dritter nach den gesetzlichen Bestimmungen über unerlaubte Handlungen zum Schadenersatz verpflichtet ist (Versicherungsfall).

EDV-System im Sinne dieser AVB ist die Gesamtheit der zur elektronischen Datenverarbeitung rechtmäßig genutzten Soft- und Hardware inklusive Daten, Datenbanken und Telefonanlagen.

Ein Eingriff im Sinne von Absatz 1 liegt vor, wenn auf das EDV-System eingewirkt wird.

Ein zielgerichteter Eingriff liegt vor, wenn sich dieser gegen eine bestimmte Anzahl von EDV-Nutzern richtet und das versicherte Unternehmen zu diesen Nutzern gehört. Versicherungsschutz besteht nicht bei einem Eingriff, der gegen eine unbestimmte Anzahl von EDV-Nutzern gerichtet ist oder gerichtet sein kann.

125

Vertrauensschadenversicherung

§ 16 Für welche unmittelbaren Schäden, verursacht durch Eingriffe Dritter in das EDV-System (Hackerschäden), besteht Versicherungsschutz, ohne dass sich ein Dritter bereichert hat?

Versicherungsschutz besteht für unmittelbare Schäden, die einem versicherten Unternehmen durch vorsätzliche, rechtswidrige und zielgerichtete Eingriffe Dritter in das EDV-System des versicherten Unternehmens (Hackerschäden) zugefügt

werden und die Schadenersatzpflicht eines Dritten nach den gesetzlichen Bestimmungen über unerlaubte Handlungen begründen, ohne dass sich ein Dritter bereichert hat (Versicherungsfall).

Bei Versicherungsfällen gemäß Absatz 1 ist unter Anrechnung auf die im Versicherungsvertrag vereinbarte Versicherungssumme für jeden Versicherungsfall die Entschädigung einschließlich sämtlicher nach diesen AVB zu erstattenden Kosten auf 50 % der Versicherungssumme, maximal EUR 1.000.000,00, begrenzt.

126

Vertrauensschadenversicherung

- Danach bestehen zwei Versicherungsfälle
 - Hat sich ein Dritter bereichert, steht die volle V-Summe zur Verfügung
 - Kann eine Bereicherung nicht nachgewiesen werden besteht V-Schutz i.H.d. Sublimits.
- In der VSV sind echte Cyber-Risiken versichert.

127

Vertrauensschadenversicherung

- CEO-Fraud-Fälle

Schäden – verursacht durch Vertrauenspersonen

§ 1 Für welche Schäden, verursacht durch eine identifizierte Vertrauensperson, besteht Versicherungsschutz?

Versicherungsschutz besteht für Schäden, die einem versicherten Unternehmen von einer identifizierten Vertrauensperson durch vorsätzliche unerlaubte Handlungen, die nach den gesetzlichen Bestimmungen zum Schadenersatz verpflichten, unmittelbar zugefügt werden (Versicherungsfall).

Eine Entschädigung setzt voraus, dass das versicherte Unternehmen den Grund und die Höhe der ihm gegenüber bestehenden Schadenersatzpflicht der Vertrauensperson nachweist.

- Nein, da Buchhalter/in nicht vorsätzlich handelt

128

Vertrauensschadenversicherung

■ Versicherungsfall nach § 10 AVB-VSV

Schäden – verursacht durch Dritte

§ 10 Für welche Schäden, verursacht durch Dritte, besteht Versicherungsschutz?

Versicherungsschutz besteht für Schäden, die einem versicherten Unternehmen von Dritten durch folgende Straftaten im Sinne des Strafgesetzbuches der Bundesrepublik Deutschland zugefügt werden:

3. Betrug

a) Gefälschte Zahlungsmittel, Schecks oder Wechsel
Versicherungsschutz besteht für Schäden durch Betrug, bei dem eine Vertrauensperson gefälschte Wechsel, Schecks oder gesetzliche Zahlungsmittel eines Mitglieds des Europäischen Wirtschaftsraums (EWR), der USA oder Kanadas für ein versichertes Unternehmen von einem Dritten entgegengenommen hat (Versicherungsfall).

b) Gefälschte Anweisung, Bestellung oder Rechnung
Versicherungsschutz besteht für Schäden durch Betrug, bei dem eine Vertrauensperson aufgrund einer von einem Dritten gefälschten Anweisung, Bestellung oder Rechnung eine Zahlung oder Warenlieferung für ein versichertes Unternehmen ausgeführt hat (Versicherungsfall).

■ Nach § 10 Abs. 3 b) AVB-VSV bis zur Entschädigungsgrenze § 13 AVB-VSV versichert (50% der VS. Max 1.Mio)

D&O-Versicherung

- Haftung der Geschäftsleitung
 - Innenregress (Unternehmen gegen Geschäftsleitung)
- Bei unzureichendem (Cyber-)Versicherungsschutz des Unternehmens:
- Nichtabschluss einer Cyberversicherung
 - Fehlerhafte Entscheidung im Rahmen der business judgment rule?
- Fehler im Risikomanagement?
 - Nichtbeschäftigung mit Datenrisiken?
 - Fehlerhafte Entscheidung im Rahmen der business judgment rule?
- Keine ausreichende fortlaufende Überwachung?
- Verstoß gegen Gesetz?
 - EU-DSGVO, BDSG, IT-Sicherheitsgesetz?

D&O-Versicherung

- Der Deckungsschutz hängt davon ab, ob ein echter Vermögensschaden entstanden ist.
- Kommt es bei der Verwirklichung von Datenrisiken nicht zu einer Beschädigung, Zerstörung oder Abhandenkommen von körperlichen Sachen (Datenträger) liegt ein Vermögensschaden vor.
- Liegt auch ein Sachschaden vor, läge ein nicht versicherter Vermögensfolgeschaden vor.
- Problem: Sind elektronische Daten Sachen i.S.d.AVB?
 - Nach Ansicht von Fortmann (r+s 2019, 688 [694]) wird der durchschnittliche VN davon ausgehen, dass ein Sachschaden i.S.e. Gebrauchsminderung bei einem leeren Datenträger vorliegt.
 - aber AVB D&O enthalten teilw. einen erweiterten Vermögensschaden. PflichtVerl. muss dann nicht für den Sach- sondern den Folgeschaden ursächlich gewesen sein.

D&O-Versicherung

- Ergebnis:
- Nichtabschluss einer Cyberversicherung
 - Deckung im Rahmen des erweiterten Vermögensschadenbegriffs
- Fehler im Risikomanagement
 - wurde durch die fehlerhafte Entscheidung eine Beschädigung, Vernichtung oder ein Abhandenkommen von verkörpert elektronischen Daten verursacht, besteht keine Deckung
- Andere Pflichtverletzungen
 - wurde durch die fehlerhafte Entscheidung eine Beschädigung, Vernichtung oder ein Abhandenkommen von verkörpert elektronischen Daten verursacht, besteht keine Deckung

Verhältnis zur Cyberversicherung

- Es kann eine Neben- oder Mehrfachversicherung bestehen.
- Eine Nebenversicherung liegt vor, wenn dasselbe Interesse gegen dieselbe Gefahr bei mehreren VR versichert worden ist, die Summe der Versicherungssummen kleiner als der Versicherungswert ist und es an einem bewussten Zusammenwirken der betroffenen VR fehlt.
- Die Mehrfachversicherung unterscheidet sich von der Nebenversicherung dadurch, dass die Versicherungssummen zusammen den Versicherungswert übersteigen oder die Summe der Entschädigungen, die von jedem einzelnen VR ohne Bestehen der anderen Versicherung zu zahlen wäre, den Gesamtschaden übersteigt.

Regelung in der Cyberversicherung

- A1-12 (AVB Cyber GDV) Vorrangige Versicherung

„Besteht Versicherungsschutz nach den Bedingungen dieses Vertrages auch in einem anderen Versicherungsvertrag, so geht die Cyberrisiko-Versicherung vor.“
- Wortlaut der Klausel stellt auf Fälle des § 78 VVG ab.
 - Außenverhältnis
 - Innenverhältnis

Subsidiaritätsklauseln

- Problematisch ist oft, dass andere relevante AVB eine Subsidiaritätsklausel enthalten. Unterschieden wird zwischen der Einfachen und der Qualifizierten
- Bsp. einfache Subsidiaritätsklausel:
 - Soweit im Versicherungsfall eine Entschädigung aus anderen Versicherungsverträgen beansprucht werden kann, gehen diese Leistungsverpflichtungen vor.
- Bsp. Qualifizierte Subsidiaritätsklausel:
 - Versicherungsschutz besteht subsidiär zu anderweitigem Versicherungsschutz: Anderweitige Leistungsverpflichtungen gehen vor, wenn für dieselbe Gefahr auch noch bei einem anderen Versicherer Versicherungsschutz besteht.

Subsidiaritätsklauseln

- Bsp. VSV: Hackerschäden sind nach § 15 AVB-VSV versichert (s.o.)
- Subsidiaritätsklausel in § 19 AVB-VSV
 - Bei Versicherungsfällen gem. §§ 15 und 16 AVB ist der Versicherungsschutz ausgeschlossen, wenn für die in §§ 15 und 16 AVB genannten Risiken ein anderer Versicherungsvertrag besteht. Dies gilt unabhängig davon, ob ein versichertes Unternehmen aufgrund des anderen Versicherungsvertrags eine Leistung beanspruchen kann.
 - Klausel dürfte m.E. einer AGB-Kontrolle nicht standhalten, da diese für Fälle der Mehrfachversicherung konzipiert ist, diese aber zugleich auch die Nebenversicherung ausschließt. Der V-Schutz wird entwertet und für die anteilig bezahlte Prämie gibt es keine Leistung.



JOHANNSEN
Rechtsanwälte

Regress

Täterregress

Ansprüche gegen die Bank

Ansprüche gegen Dienstleister

Ansprüche gegen Lieferanten

Ansprüche gegen Arbeitnehmer

07.10.2026
Die Cyberversicherung
Seite 37

137



JOHANNSEN
Rechtsanwälte

Forderungsübergang

- § 86 Abs. 1 VVG: Steht dem Versicherungsnehmer ein Ersatzanspruch gegen einen Dritten zu, geht dieser Anspruch auf den Versicherer über, soweit der Versicherer den Schaden ersetzt. Der Übergang kann nicht zum Nachteil des Versicherungsnehmers geltend gemacht werden.
- Gem. § 87 VVG ist die Vorschrift halbzwingend.
 - Kein Abweichen zum Nachteil des VN.
- VR ist aktivlegitimiert, sobald er geleistet hat.
 - Deckungsverhältnis wird im Rahmen der Aktivlegitimation nicht geprüft. D.h. Ansprüche gegen auch über wenn der VR irrtümlich geleistet hat.

07.10.2026
Die Cyberversicherung
Seite 38

138

Täterregress

Ansprüche gegen den Angreifer aus § 823 Abs. 2 BGB i.V.m.

- § 202a StGB (Ausspähen von Daten)
- § 202b StGB (Abfangen von Daten)
- § 263a StGB (Computerbetrug)
- § 303a StGB (Datenveränderung)
- § 303b StGB (Computersabotage)
- § 23 GeschGeh (Verrat von Geschäfts- und Betriebsgeheimnissen)

Ansprüche gegen den Angreifer aus § 823 Abs. 1 BGB

- Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb (DDoS-Angriff)

Gerichtsstand:

- Angriff aus dem Ausland (Art. 7 Nr. EUGVVO; Art. 6 Abs. 1 EuGVVO)
- Sind die Daten in Deutschland gespeichert – Art. 4 Abs. 1 Rom II-VO (deutsches materielles Recht)

Täterregress

- Ansprüche gegen Hilfsperson des Täters § 830 BGB
- Ansprüche gegen den Geldwäsche-Kurier (Phishing)
 - In Höhe der „Provision“ BGH Urt.v. 16.01.2018, VI ZR 474/16
 - In voller Höhe bei Bösgläubigkeit § 819 BGB, LG Kleve 28.10.2015, 1 O 202/14

Ansprüche gegen die Bank

- Oft eine Frage der Autorisierung (§ 675u S. 2 BGB)
 - Eine Autorisierung liegt gem. § 675j Abs. 1 Satz 1 BGB vor, wenn der Bankkunde dem Zahlungsvorgang zugestimmt hat. Die Zustimmung kann dabei auch über die Grundsätze der Duldungs- und Anscheinsvollmacht zugerechnet werden.
 - Wird der VN durch Schadsoftware zur Eingabe unverbrauchter TAN veranlasst, wird nach der Lit. eine Zurechnung verneint vgl. KG, MMR 2011, 338.
 - Wird der VN aufgefordert einen hohen Betrag zurück zu überweisen, liegt eine Autorisierung vor, vgl. AG Köln MMR 2013, 819.

Ansprüche gegen Lieferant

- Insbes. Gegen Hersteller der verwendeten (Sicherheits-) Software
 - Vertraglich? Regelmäßig Haftungsausschlüsse
 - Deliktische Schadensersatzansprüche denkbar insbes. Produzentenhaftung für Konstruktionsfehler.
 - Derartige Ansprüche kommen grundsätzlich in Betracht, wenn an einer anderen Sache als dem fehlerhaften Produkt selbst (z.B. an einem anderen Programm oder der Festplatte) ein Sachschaden eingetreten ist und die Produktgefahren im Zeitpunkt des Inverkehrbringens nach dem Stand von Wissenschaft und Technik vorhersehbar gewesen waren.

Ansprüche gegen Dienstleister

- Vertragliche Ansprüche gegen externen Dienstleister
 - Verletzen diese IT-Sicherheitspflichten können Anspr. Bestehen
 - Bspw. IT-Outsourcing oder Online-Banking
- Anbieter von Telemedien § 13 Abs. 7 TMG sind verpflichtet für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass ihre technischen Einrichtungen dem Stand der Technik vor unerlaubtem Zugriff geschützt sowie Datenschutzverletzungen und Störungen durch äußere Angriffe gesichert sind.

Ansprüche gegen den ArbN des VN

- Betrieblich veranlasste Tätigkeit
 - Haftung ggf. beschränkt (Innerbetrieblicher Schadenausgleich)
 - CEO-Fraud LAG Sachsen, Urt.v. 13.06.2017- 3 Sa 556/16 (150t. €)
 - Social engineering LAG Köln 31.07.2026 – 8 Sla 603/25 (50 Mio. €)
- Revision wurde eingelegt 2 AZR 164/26
- Nicht betrieblich Veranlasst
 - Volle Haftung

Ansprüche gegen Geschäftsleiter

- Vorstand § 93 Abs. 2 S.1 AktG
- Geschäftsführer § 43 Abs. 2 GmbH
- grds. Zwei Fallgruppen
 - Verstößt Geschäftsleiter selbst gegen ein Gesetz oder toleriert er ihm bekannte Verstöße? Oder
 - Wurde lediglich die allgemeine Pflicht zur Unternehmensleitung verletzt?(§ 91 Abs. 2 AktG)

145

Mehrfachversicherungsausgleich (früher Doppelversicherung)

A1-12 Vorrangige Versicherung

Besteht Versicherungsschutz nach den Bedingungen dieses Vertrages auch in einem anderen Versicherungsvertrag, so geht die Cyberrisiko-Versicherung vor.

Ein Regressanspruch nach § 78 Abs. 2 VVG bleibt davon unberührt.

146

Cyberversicherungen für Privatkunden

- Für Privatkunden werden Produkte angeboten, welche die folgenden Bausteine enthalten können:
- Cyber-Prävention
 - Insbes. IT-Assistance-Leistungen
- Cyber-Eigenschäden
 - Schutz bei Einkäufen und Verkäufen im Internet
 - Missbrauch von Zahlungsdaten
 - Missbrauch des Online-Bankings
 - Datenrettung- und Wiederherstellung
- Cyber-Haftpflicht
 - Ungewollte Übermittlung von Schadprogrammen
 - Verletzung datenschutzrechtlicher Bestimmungen
- Cyber-Rechtsschutz

147

Eigenschaden – Bsp. Debeka AVB-C Stand 01.04.2025

Versichert ist, im Zusammenhang mit Ihren Privatkonten, z. B. der Missbrauch

- Ihrer privat genutzten Zahlungskarte (z. B. EC-Karte/Girokarte, Debitkarte, Kreditkarte oder Kundenkarte mit Zahlungsfunktion),
- Ihrer Karten-/Kontodaten bei (Online-)Bezahlvorgängen,
- beim bargeldlosen Bezahlen von Waren und Dienstleistungen sowie kontaktlosen Bezahlen (mittels sogenannter Near Field Communication NFC),
- bei Abhebungen an Geldautomaten z. B. durch manipulierte Kartenlesegeräte (Ausspähen von Kartendaten und PIN, Skimming),
- beim Telefon-Banking,
- bei Lastschriftverfahren, Überweisungsaufträgen und Scheckeinzahlungen,
- beim Online-Banking oder E-Payment (Nutzung sonstiger Online-Bezahlsysteme mit Bank-Funktion, z. B. PayPal, Apple-Pay): Ein Dritter verschafft sich rechtswidrig während Ihres Online-Bankings bzw. Online-Bezahlvorgangs am eigenen Laptop/PC oder mobilen Endgerät (z. B. Tablet, Smartphone) Ihre persönlichen Daten,

148

Eigenschaden

- durch Phishing: Mithilfe gefälschter Kommunikation in Textform (z. B. E-Mails, SMS, Webseiten) verschafft sich ein Dritter rechtswidrig Ihre vertraulichen Zugangs- und/oder Identifikationsdaten. Dies geschieht, indem Sie zu einer Handlung aufgefordert werden (Anklicken eines Links, Öffnen von Anhängen etc.). Anschließend begeht der Dritte unter Ihrer Identität betrügerische Aktivitäten meist finanzieller Art oder greift auf andere Online-Konten zu. Mehrere Schäden stellen hierbei einen Versicherungsfall dar, wenn sie auf einem Phishing-Angriff beruhen, bei dem der Dritte mehrere Zugangs- und Identifikationsdaten von Ihnen erlangt hat,
- durch Pharming: Sie werden auf eine betrügerische Webseite umgeleitet. Dort geben Sie arglos Ihre Daten ein. Ein Dritter erfasst die eingegebenen sensiblen Informationen wie Benutzernamen, Passwörter, Kreditkartendaten etc. Anschließend begeht der Dritte unter Ihrer Identität betrügerische Aktivitäten meist finanzieller Art oder greift auf andere Online-Konten zu. Mehrere Schäden stellen hierbei einen Versicherungsfall dar, wenn sie auf einem Pharming-Angriff beruhen, bei dem der Dritte mehrere Zugangs- und Identifikationsdaten von Ihnen erlangt hat.

Eigenschaden

C 3.2 Welche Kosten übernehmen wir?

Wir erstatten Ihren Vermögensschaden bis maximal 20.000 Euro pro Versicherungsjahr. Voraussetzung ist, dass die Bank, der Kreditkarten- oder Zahlungskartenherausgeber, der Zahlungsdienstleister oder ein sonstiges Geldinstitut die Erstattung des Schadens (vollständig oder teilweise) rechtmäßig schriftlich abgelehnt hat – z. B., weil Sie Ihre Pflichten diesen gegenüber verletzt haben. Diese müssen den Sitz in Deutschland haben.

Drittschäden

D 2.1.1 Ungewollte Übermittlung von Schadprogrammen

Versichert sind Haftpflichtansprüche wegen Schäden aus der ungewollten Übermittlung von Schadprogrammen (inkl. Spamming/Cookies) durch das Bereitstellen, die Versendung oder den Austausch elektronischer Daten zwischen Ihnen und dem Geschädigten.

Das gilt auch dann, wenn Sie über ein privates mobiles Endgerät Zugriff auf ein beruflich genutztes Betriebssystem haben und hierüber Schadprogramme in ein solches Betriebssystem übermittelt werden.

Drittschäden

D 2.1.2 Verletzung datenschutzrechtlicher Bestimmungen

Versichert sind Haftpflichtansprüche wegen Schäden aus der Verletzung von Datenschutzgesetzen durch Verarbeitung personenbezogener Daten.

Als Verarbeitung gilt jeder – mit oder ohne Hilfe automatisierter Verfahren ausgeführte – Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten. Dazu zählen das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung der Daten.

Versichert sind auch gesetzliche Haftpflichtansprüche wegen Schäden von Versicherten (Versicherungsnehmer oder mitversicherte Personen) untereinander. Der Ausschluss in Abschnitt D 5.3 findet insoweit keine Anwendung.

Drittschäden

D 2.1.3 Verletzung urheberrechtlicher Bestimmungen

Versichert sind Haftpflichtansprüche, die aus einer unerlaubten Nutzung oder Verwertung von urheberrechtlichen geschützten Werken im Internet entstehen. Dabei übernehmen wir auch die Gebühren einer Abmahnung, mit der ein Anspruch auf Unterlassung oder Widerruf gegen Sie begehrt wird.

Nicht versichert sind hingegen

- Ansprüche, wenn Sie die fehlende Berechtigung zu der Veröffentlichung kannten.
- Vertragsstrafen sowie Bußgelder und Strafen aus einer strafrechtlichen Verfolgung einer Urheberrechtsverletzung.

Cyberversicherungen für Privatkunden

- Keine Musterbedingungen des GDV
- Entschädigungsleistungen sind stark limitiert (drei-, vier- und selten fünfstellige Leistungen versichert)
- Versicherungsschutzniveau ist i.d.R. deutlich höher als in zusätzlichen Deckungsbausteinen der Hausrat-, Privathaftpflicht- und Rechtsschutzversicherung.

Phishing in der Hausratversicherung (Bsp. Allianz Komfort 10/2019)

2.3.2 Internetschutz

2.3.2.1 Zahlungsverkehr im Internet

Sie sind geschützt, wenn durch eine der nachfolgend genannten Gefahren ungewollte Zahlungen von Ihrem Konto aus vorgenommen werden.

Unter Konto verstehen wir:

- Ihre Konten
- Ihre Depots
- Ihre anderen virtuellen Konten, von denen Zahlungen an Dritte ausgeführt oder Zahlungen von Dritten empfangen werden können (beispielsweise "PayPal")

Voraussetzung ist, dass Sie diese Konten bei Geldinstituten oder Online-Bezahldiensten in einem der folgenden Länder unterhalten:

- in einem Land der Europäischen Union (EU)
- in der Schweiz, in Norwegen, Island, Liechtenstein

Bitte beachten Sie: Wir ersetzen Ihnen den entstandenen Vermögensschaden, maximal jedoch 10.000 Euro je Versicherungsfall.

Phishing in der Hausratversicherung (Bsp. Allianz Komfort 10/2019)

Versicherte Gefahren	Was ist das genau?
"Phishing" und "Pharming"	"Phishing": Dritte gelangen über eine gefälschte E-Mail an die Zugangs- und Identifikationsdaten zu Ihrem Konto. "Pharming": • Dritte ahmen den Internetauftritt Ihres Geldinstituts/Online-Bezahldienstes nach und leiten dadurch Ihre Anfrage auf eine betrügerische Seite um. • Sie führen im Glauben an die Echtheit der Seite Zahlungsvorgänge aus.
"Trojaner" oder "Keylogger"	Sonstiges Ausspähen von Zugangsdaten ("Trojaner" oder "Keylogger"): • Dritte gelangen mittels verdeckt operierender Schadprogramme auf Ihrem Computer an die Zugangs- und Identifikationsdaten zu Ihrem Konto. • Mithilfe dieser Daten führen diese Dritten dann nicht autorisierte Zahlungsvorgänge aus.
Fehlerhafte Eingaben bei Online-Überweisungen	Versichert ist auch Folgendes: • Sie geben bei einer Online-Überweisung Daten fehlerhaft ein. • Dadurch veranlassen Sie irrtümlich die Gutschrift auf dem Konto eines Dritten. Voraussetzung ist, dass Sie und Ihr Geldinstitut bzw. Online-Bezahldienst vergeblich versucht haben, den überwiesenen Betrag vom Zahlungsempfänger bzw. von der Zahlungsempfängerin zurückzuerlangen.
Entwendung von Online-Banking-Zugangsdaten bei Wohnungseinbruch	Versichert ist auch Folgendes: • Dritte brechen in die versicherte Wohnung ein. • Dabei entwenden oder kopieren sie die Zugangsdaten zu Ihren online geführten Konten. • Mithilfe dieser Daten führen diese Dritten dann nicht autorisierte Zahlungsvorgänge aus.

LG Hamburg zu Phishing- und Pharming, Urt. v. 12.12.2024

■ Sachverhalt:

- Die Klägerin trägt vor Opfer eines Betruges geworden zu sein, der nach der versicherten Gefahr der Bekl. „Internetschutz“ versichert sei. Sie hat auf der Internetplattform e. Kleinanzeigen einen Kosmetikartikel zum Verkauf angeboten. Es habe sich eine angebliche Erwerberin gemeldet, die über ein neues Bezahlsystem von e. Kleinanzeigen habe bezahlen wollen. Die Klägerin hat dann der vermeintlichen Erwerberin ihre Mobilnummer mitgeteilt. Daraufhin hat sie eine SMS zur Verifizierung nebst einem Code erhalten. Die Klägerin hat den Link angeklickt und ihre Debitkarteninformationen der D. Bank auf der Website eingegeben. Die Klägerin sei dann auf eine Website geleitet worden, welche ähnlich der D.Bank gestaltet war. Sie hat dann einen weitere SMS der vermeintlichen D.Bank erhalten und auf der gefakten Seite der D. Bank eingegeben. Dadurch wurde eine Neukopplung des TAN-Geräts ausgelöst und ein Betrag i.H.v. 5.600 € abgebucht.

LG Hamburg zu Phishing- und Pharming, Urt. v. 12.12.2024

■ Entscheidung des LG Hamburg:

1. Bei einem „**Phishing**“ im Sinne der im Streitfall vereinbarten AVB müssen Dritte über eine gefälschte E-Mail an die Zugangs- und Identifikationsdaten für das Konto des VN gelangt sein. Eine andere elektronische Kontaktaufnahme, etwa per SMS oder über eine Internetseite, reicht nicht aus.
2. Ein bedingungsgemäßes „**Pharming**“ setzt u. a. voraus, dass der VN im Glauben an die Echtheit einer in Wahrheit gefälschten Internetseite Zahlungsvorgänge ausführt. Es genügt nicht, wenn er lediglich meint, seine Eingabe diene allein dazu, sich bei einem Bezahlsystem anzumelden.

LG Berlin II zu Phishing in VHB2016, Urt.v. 27.05.2025, 24 O 250/24

■ Sachverhalt:

- Die Klägerin behauptet, Dritte hätten sich Zugang zu ihrem Online-Bankkonto bei der Berliner Sparkasse verschafft. Am 07.07.2023 habe sie von einer Kontaktnummer der xxxxx, von der sie auch zuvor SMS-Nachrichten erhalten habe, eine SMS mit einem Link an ihre Handynummer geschickt bekommen. Später am selben Tag habe sie jemand angerufen, der sich als Mitarbeiter der xxxxx ausgegeben und ihr gesagt habe, sie müsse zur Verlängerung des ablaufenden pushTAN-Verfahrens auf den Link in der SMS klicken. Die Klägerin habe dies getan. Anschließend hätten die Täter ohne Wissen und Zutun der Klägerin eine Mobile Pay-App freigeschaltet und damit die streitgegenständlichen Bezahlvorgänge vorgenommen.

LG Berlin II zu Phishing in VHB2016, Urt.v. 27.05.2025, 24 O 250/24

■ Bedingungslage:

- Versichert sind Vermögensschäden, sofern unberechtigte Dritte sich im Internet Zugangs- und Identifikationsdaten zum privat genutzten Bankkonto des Versicherungsnehmers (...) verschafft haben und mit diesen Daten unberechtigter Weise Überweisungen vom Bankkonto vornehmen.

LG Berlin II zu Phishing in VHB 2016, Urt.v. 27.05.2025, 24 O 250/24

■ Entscheidung:

- Das LG Berlin II hat die Klage abgewiesen. Die Klage war unschlüssig. Der Anspruch nach Ziffer A.1.1 Klausel 0991 VHB 2016 setzt voraus, dass sich unbekannte Dritte im Internet Zugangs- und Identifikationsdaten zum privat genutzten Bankkonto des Versicherungsnehmers verschafft haben und mit diesen Daten unberechtigter Weise Überweisungen vom Bankkonto vorgenommen haben. Es kann dahin stehen, auf welche konkrete Weise sich die Täter Zugang zum Bankkonto der Klägerin verschafft haben. Denn es wurden keine Überweisungen im Sinne der einschlägigen Klausel vorgenommen. Dies ergibt eine Auslegung der Klausel.



Christoph König
Rechtsanwalt | Partner
Versicherungskaufmann



christophkoenig@kanzlei-
johannsen.de



www.kanzlei-johannsen.de
Tel. 030 – 20 91 73 01