VERSICHERUNGS KAMMER BAYERN

Ein Stück Sicherheit.

CYBER-VERSICHERUNG

# Unser Schutzschirm für Ihr digitales Arbeiten.

Mit unserer CyberSchutz-Versicherung ist Ihr Unternehmen digital gut aufgestellt und gut geschützt.

Finanzgruppe

# Mit unserer Cyber-Versicherung den Erfolg Ihrer Digitalisierung sichern.

### DIGITALISIERUNG BIRGT RISIKEN

Ob Kundendaten, vertrauliche betriebliche Informationen oder Steuerung der internen Prozesse – beruflich und geschäftlich bewegen sich Unternehmen, ihre Vertreter sowie Mitarbeiter permanent in der digitalen Welt – im Cyberspace. Durch die steigende Professionalität und Internationalität der Cyberangriffe erhöhen sich die Angriffe und Attacken auf digitale Systeme und Daten rasant.

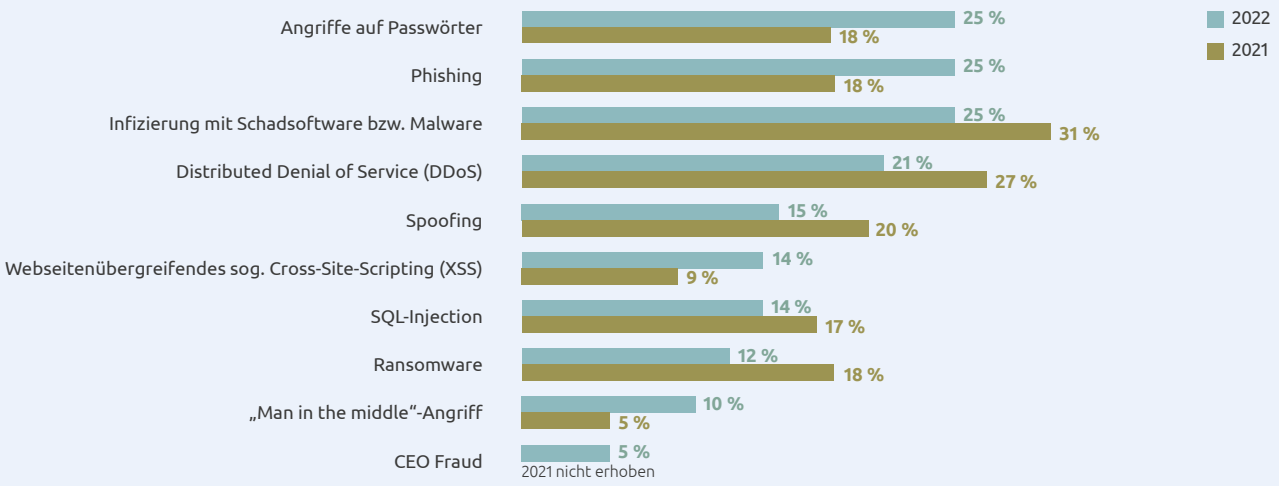
### CYBERANGRIFFE KÖNNEN DIE EXISTENZ IHRES UNTERNEHMENS BEDROHEN

Der deutschen Wirtschaft entsteht ein jährlicher Schaden von rund 203 Milliarden Euro durch Diebstahl von IT-Ausrüstung und Daten, Spionage und Sabotage. 45 Prozent der Unternehmen meinen, dass Cyberattacken ihre geschäftliche Existenz bedrohen können – vor einem Jahr lag der Anteil bei gerade einmal 9 Prozent.
(Quelle: Digitalverband Bitkom)

Über 70 Prozent der Unternehmen ergriffen Maßnahmen zur Verbesserung ihrer Cybersicherheit. Dennoch kann keine technische oder organisatorische Maßnahme eine 100-prozentige Sicherheit garantieren.

## WELCHE CYBERRISIKEN GIBT ES?

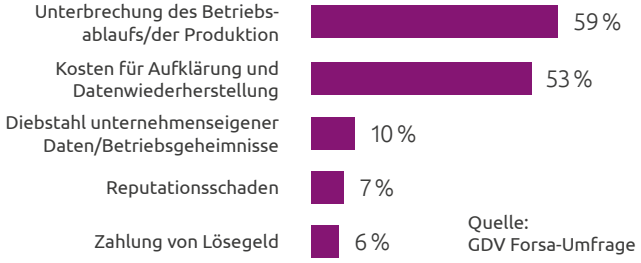
**Welche der folgenden Arten von Cyberangriffen haben innerhalb der letzten 12 Monaten in Ihrem Unternehmen einen Schaden verursacht?**




Quelle: Bitkom Research 2022

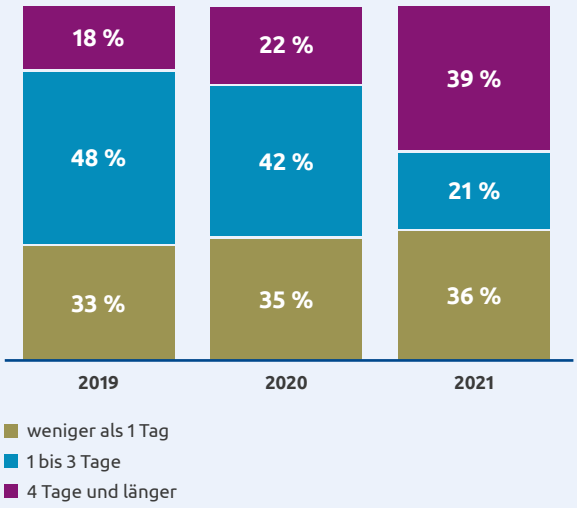
## DIE SCHÄDEN

Die Attacken führten zu wirtschaftlichen Schäden durch ...[1]




## CYBERATTACKEN LEGEN UNTERNEHMEN LÄNGER LAHM

**Wie lange hat es gedauert, die IT-Systeme wiederherzustellen und die Schadsoftware zu beseitigen?**




Quelle: Repräsentative Forsa-Befragung von 300 Entscheidern in kleinen und mittleren Unternehmen im April 2021

## DIE CYBER-VERSICHERUNG SCHÜTZT

Unsere CyberSchutz-Versicherung schützt Ihr Unternehmen vor finanziellen Risiken, die als Folge von Verletzungen der IT-Sicherheit und Cyberangriffen entstehen können. Sie umfasst Haftpflichtansprüche, Vertrauensschäden (Taten mit Vorsatz), Assistance-Leistungen (Forensik, Datenwiederherstellung) und optional auch Ertragsausfall.

## IHRE VORTEILE

- Optionale Auswahlmöglichkeit für den maßgerechten Versicherungsschutz
- Versicherungsschutz für gezielte und ungezielte Cyberangriffe
- Versicherungsschutz auch für elektronische Daten und informationsverarbeitende Systeme, die der Versicherungsnehmer in einer Cloud und/oder bei einems externer Dienstleister nutzt
- Versicherungsschutz bei Cybersicherheitsverletzungen durch jedwede Art von Schadsoftware
- Versicherungsschutz für Eigenschäden, auch durch vorsätzliche Cyber-/Datensicherheitsverletzung durch Mitarbeiter und Vertrauenspersonen wie Rechtsanwälte und Steuerberater (die im Auftrag des versicherten Unternehmens für dieses tätig sind)
- Versicherungsschutz für die Vertragsstrafen nach PCI-DSS-Standard
- Versicherungsschutz für Kosten von Straf- und weiteren Verfahren (die im Zusammenhang mit einem Haftpflichtanspruch entstehen)
- Versicherungsschutz für die Betriebsunterbrechung infolge eines Bedienfehlers, der zur Beschädigung/Zerstörung/Unbrauchbarkeit von Daten führt
- Versicherungsschutz auch bei Verletzung datenschutzrechtlicher Bestimmungen, die VOR Vertragsbeginn begangen wurden, ohne zeitliche Einschränkung (sofern diese zum Zeitpunkt des Vertragsabschlusses nicht bekannt waren)
- Cyber-Schadenservice. Die Hotline unseres IT-Dienstleisters steht rund um die Uhr, 7 Tage die Woche und 365 Tage im Jahr, schon bei einem Cyberverdachtsfall, zur Verfügung.
- Cyber Schulung & Prävention. Aufmerksame und geschulte Mitarbeiter sind der beste Schutz vor Cyberschäden. Nutzen Sie unser kostenfreies Angebot um sich, Ihre Mitarbeiter und auch Ihre IT Welt auf den neusten Stand zu bringen.

# Unsere Serviceleistungen für Ihre Cybersicherheit.

| Leistung | CyberSchutz | CyberSchutz Plus |
|---|---|---|
| **Haftpflicht-Vermögensschaden** | | |
| › Prüfung der Haftpflichtfrage | ✓ | ✓ |
| › Verletzung von Datenschutzgesetzen | ✓ | ✓ |
| › Vertraulichkeitsverletzung | ✓ | ✓ |
| › Vertragsstrafen (PCI-Strafen) | ✓ | ✓ |
| › Strafverteidigungskosten | ✓ | ✓ |
| **Vertrauensschaden und Erpressungsversicherung** | | |
| › Unmittelbarer Eigenschaden infolge Datensicherheitsverletzung | ✓ | ✓ |
| › Kosten und Serviceleistungen (wie Eigenschaden) | ✓ | ✓ |
| › Cybererpressung | ✓ | ✓ |
| **Eigenschaden – Kosten und Serviceleistungen** | | |
| › Wiederherstellung von Daten und Software | ✓ | ✓ |
| › IT-forensische Untersuchungen einschließlich Empfehlungen | ✓ | ✓ |
| › Beratungskosten (Rechts- und Krisenberatung) | ✓ | ✓ |
| **Ertragsausfall** | | |
| › Entgangener Betriebsgewinn und fortlaufende Kosten | ✗ | ✓ |
| › Auch bei Bedienfehlern | ✗ | ✓ |
| › Kosten und Serviceleistungen (wie Eigenschaden) | ✗ | ✓ |
| › Ausfall des Clouddienstleisters durch DDoS-Angriff | ✗ | optional |

## Zusammen mit unserem Dienstleister Perseus unterstützen wir Sie mit Schulungs- und Präventionsangeboten

| Leistung | CyberSchutz | CyberSchutz Plus |
|---|---|---|
| **Cyber Schulung & Prävention*** | | |
| › **E-Learning Cybersicherheit/Phishing/Datenschutz**: Es werden Schulungen zu verschiedenen Themen angeboten, um Sie und Ihre Mitarbeitenden zu sensibilisieren. Unter anderen finden Sie Online-Trainings zum Thema Phishing sowie Cybersicherheit & Datenschutz. Die Schulungen sind in Deutsch, Englisch und Spanisch verfügbar. | ✓ | ✓ |
| › **Regelmäßige Phishing-Kampagnen**: In Zusammenarbeit mit unserem Dienstleister können Sie Ihre Mitarbeiten testen. Mit simulierten Betrugs-E-Mails wird das Gefahrenbewusstsein Ihrer Mitarbeitenden kontinuierlich überprüft. Hierbei können Sie erkennen, wie sehr Ihre Mitarbeitenden bereits sensibilisiert sind. | ✓ | ✓ |
| › **E-Mail-Scanner für verdächtige E-Mails**: Zur Verwendung für alle Ihre Mitarbeitenden ist im Werkzeugkasten unseres Dienstleisters Perseus die E-Mail-Adresse im Malware-Scanners hinterlegt. Einfach verdächtige E-Mail weiterleiten und in wenigen Minuten erfahren, ob Dateianhänge gefährlich oder unbedenklich sind. Denken Sie daran: 70 % der erfolgreichen Cyberangriffe erfolgen durch E-Mails. | ✓ | ✓ |
| › **Datensicherheits-Check für E-Mail-Adressen** | ✓ | ✓ |
| › **Darknet-Scan für die Unternehmensdomain** | ✓ | ✓ |
| › **Browser-Check** | ✓ | ✓ |
| › **Gefahrenwarnung vor aktuellen Angriffen**: Regelmäßig sorgen Hacker-Attacken, Datendiebstähle, Sicherheitslücken oder andere Cybervorfälle für Risiken in der digitalen Welt. Damit Sie rechtzeitig über mögliche neue Gefahren Bescheid wissen, gibt es die Perseus-Gefahrenwarnung. | ✓ | ✓ |
| › **IT-Sicherheitsprüfung**: Mit der interaktiven Checkliste unseres Dienstleisters Perseus erhalten Sie schnell einen Überblick über den aktuellen Sicherheitsstatus Ihres Unternehmens und erfahren, welche Schritte Sie aktiv und mit Unterstützung durch Perseus vornehmen sollten, um Ihre Sicherheit sofort zu verbessern. | ✓ | ✓ |
| › **Checklisten, Blog, Newsletter & Glossar** | ✓ | ✓ |
| **Cyber Schadenservice**** | | |
| › **24-h-Notfallhilfe**: Vom Verdachtsfall über Abwehr bis zur Dokumentation – unsere Dienstleister Deutsche Assistance und CYCO unterstützen Sie rund um die Uhr – auch beim kleinsten Verdacht auf einen Cyberangriff. Per Telefon, E-Mail und (falls notwendig) via Fernwartung. | ✓ | ✓ |
| › **Cyber Security Expert Desk** | ✓ | ✓ |
| › **Identifizieren der Angriffsquelle** | ✓ | ✓ |
| › **Definieren von Gegenmaßnahmen** | ✓ | ✓ |
| › **Koordination und Übergabe an Vor-Ort-Team** | ✓ | ✓ |
| › **Erforderliche Maßnahmen zur Schadensminderung** | ✓ | ✓ |
| › **Beratung des Geschädigten hinsichtlich Meldepflichten** | ✓ | ✓ |
| › **Alarmierung des Cyberintervention Teams** | ✓ | ✓ |

* Die Cyber Schulungs- & Präventionsangebote sind freiwillige Leistungen die vom Bayerischer Versicherungsverband Versicherungsaktiengesellschaft (BVV) zusammen mit unserem Dienstleister Perseus erbracht werden. Der BVV behält sich eine Änderung oder Wegfall des Dienstleister oder der Leistungen vor. Der Versicherungsschutz ist dadurch nicht berührt.

** Der Cyber-Schadenservice wird von unseren Partnern Deutsche Assistance und CYCO zur Verfügung gestellt. Alle im Cyber Schadenservice enthaltenen Leistungen stehen ohne Anrechnung auf Versicherungssumme und ohne Selbstbehalt für 48 Stunden zur Verfügung.

# Wenn eine E-Mail die Existenz bedroht: Beispiele für Cyberangriffe.

HAFTPFLICHT-VERMÖGENSSCHADEN

## E-Mail an falschen Verteiler geschickt

Eine Arzthelferin schickt versehentlich Informationen über Patientenabrechnungen statt an die Krankenkasse an einen externen E-Mail-Verteiler. Dadurch werden die Vorschriften der neuen DSGVO verletzt. Der Arzt muss alle betroffenen Patienten sowie die zuständige Datenschutzbehörde informieren. Die betroffenen Patienten können Schadenersatzansprüche wegen Datenverletzung erheben. Zudem ist die Beratung durch eine Fachanwaltskanzlei erforderlich.

**Als Versicherung übernehmen wir die notwendigen Beratungshonorare sowie die Kosten für Information und Reputationswiederherstellung. Außerdem die Kosten bei Rechtsstreitigkeiten mit betroffenen Patienten sowie den berechtigten Schadenersatz.**

VERTRAUENSSCHADEN UND ERPRESSUNGSVERSICHERUNG

## Diebstahl von Firmenvermögen

Ein Mitarbeiter in der Buchhaltung öffnet versehentlich einen E-Mail-Anhang, der ein Schadprogramm enthält. Mittels diesem gelingt es Unbekannten, die Bankzugangsdaten zu erlangen und 200.000 EUR von den Firmenkonten ins Ausland zu überweisen.

**Wir bezahlen den entstandenen eigenen Vermögensschaden des Versicherungsnehmers, somit auch die Kosten für die IT-forensischen Untersuchungen, Überwachung von Girokonten, Wiederherstellung von Daten und Software sowie für Beratung und Krisenmanagement.**

EIGENSCHADEN

## Hacker erbeuten Kreditkartendaten

Unbekannte verschaffen sich mittels eines Schadprogramms rechtswidrig Zugang zum online-basierten Abrechnungssystem für Kreditkarten eines Hotels. Dabei werden über 10.000 Kreditkartendaten von Hotelgästen gestohlen und unrechtmäßig genutzt.

**Wir übernehmen die Prüfung und Erfüllung berechtigter Schadenersatzansprüche der Kreditkarteneigentümer. Zudem die Kosten für die gesetzlichen Informationspflichten nach der neuen DSGVO, die Vertragsstrafe wegen Verletzung des öffentlichen Payment Card Industrie(PCI)-Datensicherheitsstandards sowie die Kosten der IT-forensischen Untersuchungen, Überwachung von Kredit- und Girokonten, die Rechtsberatungskosten, Krisenmanagement und Öffentlichkeitsarbeit wie auch die Wiederherstellung von Daten.**

ERTRAGSAUSFALL

## Betriebsstillstand durch Hackerangriff

Ein mittelständischer Betrieb, der seine Produktion mittels IT steuert, wird Opfer eines Hackerangriffs. Dem Angreifer gelingt es, die IT für 5 Tage lahmzulegen und viele Daten zu zerstören. Der Betrieb erleidet einen Ertragsausfallschaden und muss das System durch einen externen Dienstleister komplett neu wiederherstellen lassen.

**Wir bezahlen den im Rahmen der CyberSchutz Plus entstandenen Betriebsunterbrechungsschaden sowie die Kosten für die IT-forensischen Untersuchungen, Wiederherstellung von Daten und Software wie auch Beratungs- und Krisenmanagementkosten.**

# Sorgen Sie bestmöglich vor.

| Wichtige Empfehlungen für Ihre Cybersicherheit | |
|---|---|
| E-Mails vor dem Öffnen prüfen (Absender, Betreff, Anhang) | ✓ |
| E-Mails vor dem Versand verschlüsseln | ✓ |
| Verwenden mehrerer Authentifizierungsmethoden | ✓ |
| Aktivieren Sie HTTPs auf Ihrer Website (HTTPs-Websites haben auf Servern ein SSL/TLS-Zertifikat installiert. Dieses verschlüsselt alle Daten und schützt | ✓ |
| Verwenden Sie je Account unterschiedliche und starke Passwörter | ✓ |
| Automatische Updates für Hard- und Software | ✓ |
| Halten Sie Ihre Software (insbesondere Betriebssystem, Firewall und Virenscanner) immer auf dem neuesten Stand | ✓ |
| Halten Sie Sicherungskopien aller Daten getrennt von Ihrem Computersystem bereit | ✓ |
| Regelmäßige Schulung/Information der Mitarbeiter über Cybergefahren (z. B. unbekannte Anhänge in E-Mails) | ✓ |
| Sicheren Zugang auf die Unternehmens-IT auch im Homeoffice bereitstellen (z. B. VPN) | ✓ |

## TIPPS FÜR DIE ERSTELLUNG EINES NOTFALLPLANS BEI CYBERATTACKEN

1. Erstellen von Handlungsrichtlinien für Mitarbeiter
2. Benennung eines für Cyber-Fragen verantwortlichen Mitarbeiters als Ansprechpartner im Falle eines Cyberangriffs
3. Liste wichtiger Fachleute mit allen Telefonnummern: IT-Leiter, IT-Dienstleister, Datenschutzbeauftragter
4. Organisation: Wer ist für was zuständig (Aufgabenverteilung)?
5. Übersicht für Datenspeicherung: Welche Daten werden wo in welchen zeitlichen Intervallen gespeichert?
6. Inhaltsverzeichnis der gespeicherten Datensicherungen: exakte Datenbeschreibung, Stand/Datum der Absicherung

## BESCHÜTZEN IST UNSERE LEIDENSCHAFT.

Weil ihm der Schutz der Menschen am Herzen lag, gründete König Max I. vor mehr als 200 Jahren eine Versicherung. Seitdem stehen wir ein Leben lang verlässlich an der Seite unserer Kunden und sorgen für die persönliche Absicherung und Vorsorge unter dem blauen Schirm. Und sind als bayerischer Versicherer wie kein anderer mit der Region verbunden.

An erster Stelle steht immer das Wohlergehen unserer Kunden. Ihre Wünsche und Bedürfnisse sind unser wichtigstes Anliegen.

Dass sich die Menschen bei uns bestens aufgehoben fühlen, sieht man an unserem Erfolg: Wir sind Marktführer in Bayern und der Pfalz und erfreuen uns seit Jahren stetigen Wachstums.

**Versicherungskammer Bayern**
**Maximilianstraße 53 · 80530 München**
**www.vkb.de**

338032; 09/23