Genossenschaftliche FinanzGruppe
Volksbanken Raiffeisenbanken

CyberCrime

Die Gefahr kommt aus dem Netz

Referent: Oliver Boselli

R+V

Du bist nicht allein.

Cyberkriminalität nimmt weiter zu
Medien berichten täglich über Attacken

„Nach einem Hackerangriff auf die **Hotelkette Motel One** sind laut einem Medienbericht Millionen Namen und Reisedaten von Kunden im Internet gelandet. Darunter auch Kreditkartendaten.“

„Continental-Mitarbeiter nutzt **nicht autorisierten Browser** und ermöglicht so den gigantischen Cyberangriff
Handelsblatt“

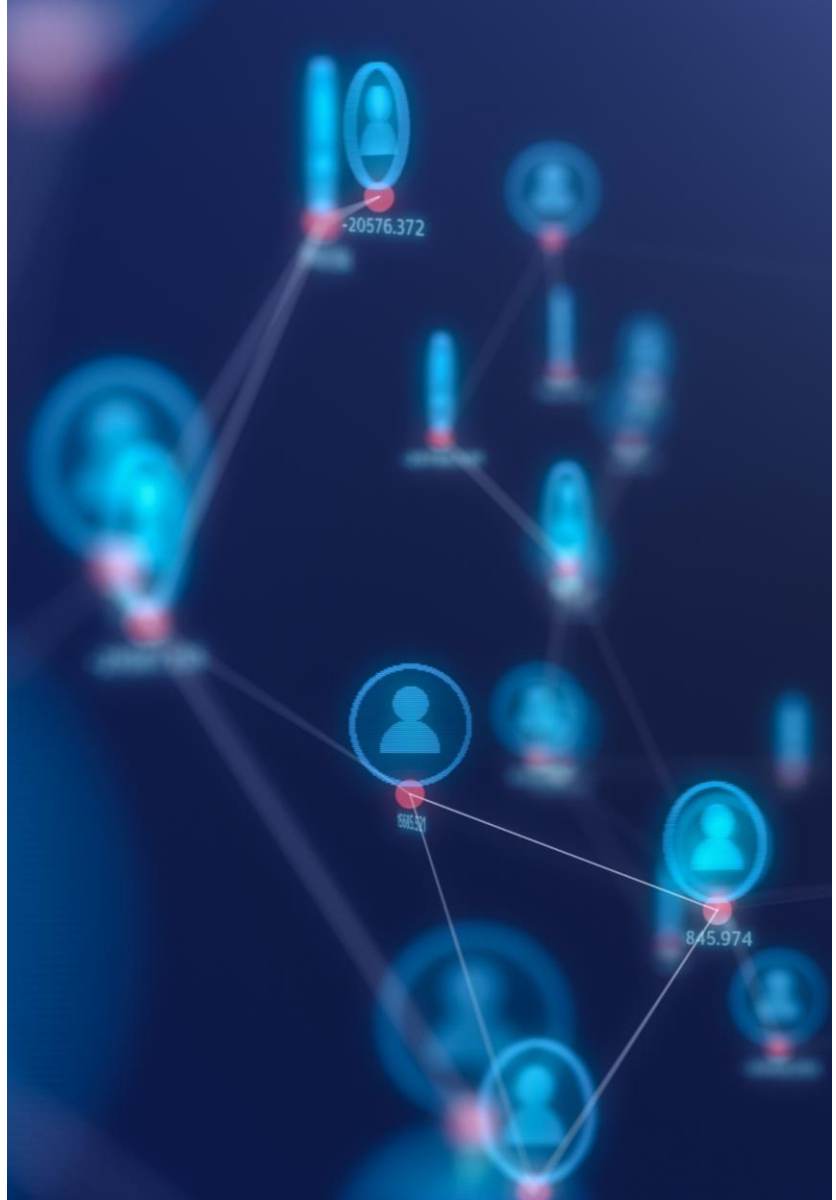
„Cyberattacke auf IT-Dienstleister Adesso: **Systeme kompromittiert, Daten kopiert**
heise online“

„Cyberangriff auf den Fahrzeug-Zulieferer Fritzmeier: **Internet, Telefon und Maschinen lahmgelegt**
Merkur“

Wenn selbst große Unternehmen es nicht schaffen, ihre Systeme zu schützen, wird es mittelständischen Firmen erst recht nicht gelingen.

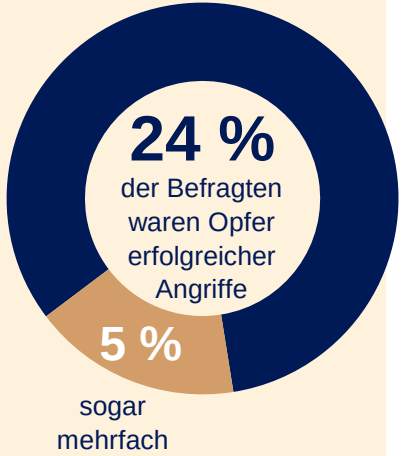
Durch die zunehmende Digitalisierung, sind Unternehmen verstärkt dem Risiko ausgesetzt, „Opfer“ ihrer eigenen Vernetzung zu werden.

Wie sicher ist Ihre IT???



Jedes vierte Unternehmen bereits betroffen

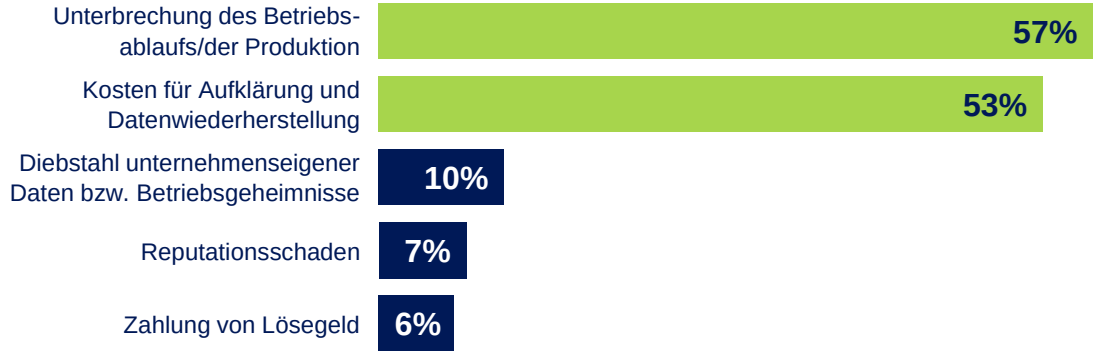
Wurde Ihr Unternehmen durch Cyberangriffe geschädigt?



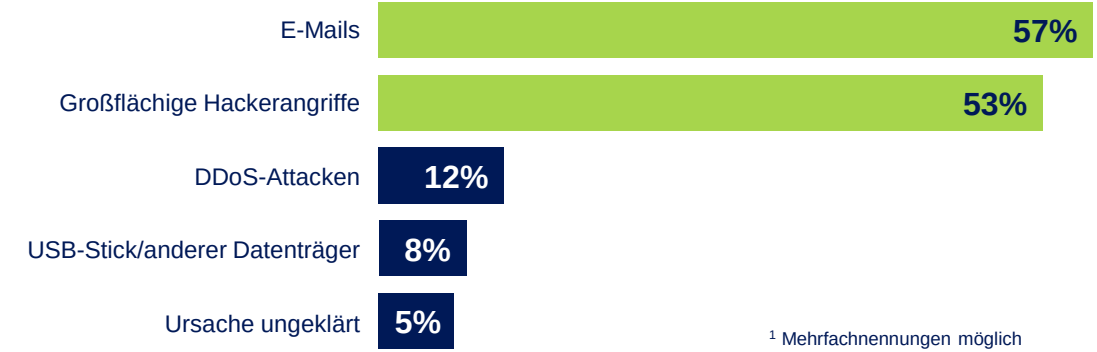
Quelle: Forsa-Umfrage „Cyberrisiken im Mittelstand“

Es gibt keine 100% Sicherheit!

Welche Schäden sind im Unternehmen durch den Cyberangriff entstanden?

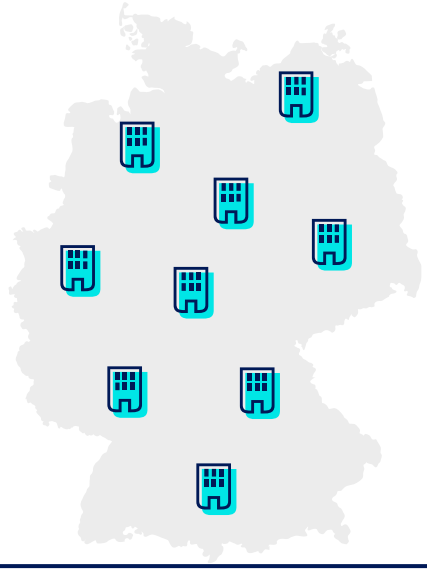


Erfolgreiche Cyberangriffe erfolgten durch …[1]



[1] Mehrfachnennungen möglich

„Das Risiko gibt es – aber…



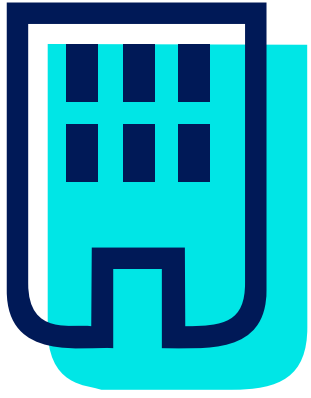
Zustimmung

75 %

Das **Risiko** von Cyberkriminalität für **mittelständische Unternehmen** in Deutschland **ist hoch.**

Zustimmung

36 %



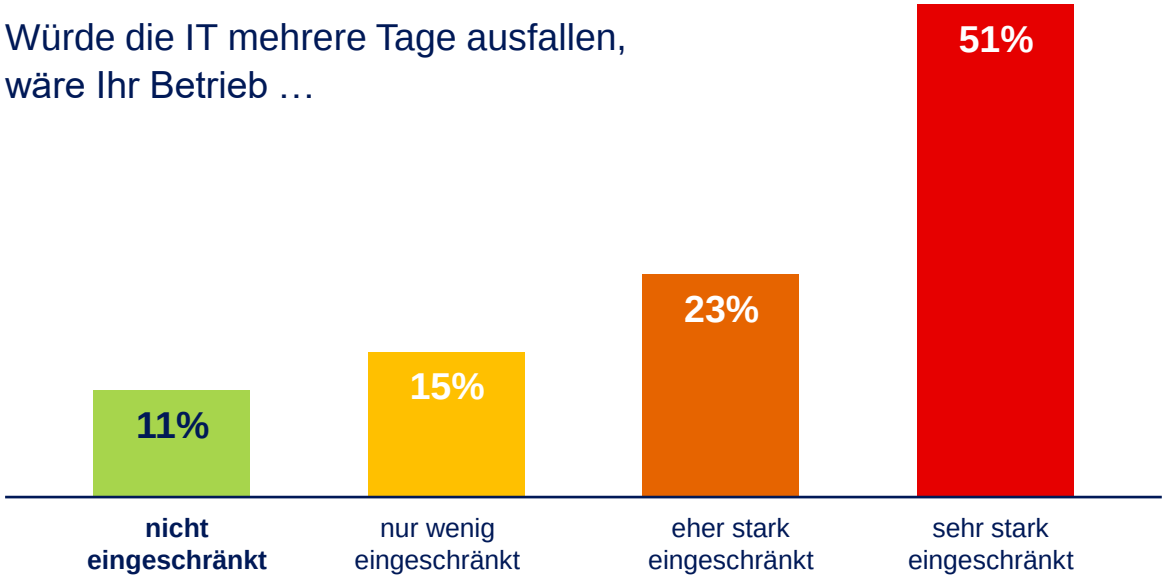
Das **Risiko** von Cyberkriminalität für das **eigene Unternehmen** in Deutschland **ist hoch.**

Quelle: Repräsentative forsa-Umfrage im Auftrag des GDV unter Entscheidern in kleinen und mittleren Unternehmen mit einem Umsatz von bis zu 50 Millionen Euro I
Grafik: www.gdv.de I Gesamtverband der Deutschen Versicherungswirtschaft (GDV)

Was passiert, wenn die IT stillsteht?

Eine nicht funktionierende Unternehmens-IT führt schnell zum Stillstand im eignen Betrieb.

Würde die IT mehrere Tage ausfallen, wäre Ihr Betrieb …



Nur 11 % geben an, dass ihr Unternehmen ohne IT gar nicht eingeschränkt wäre.

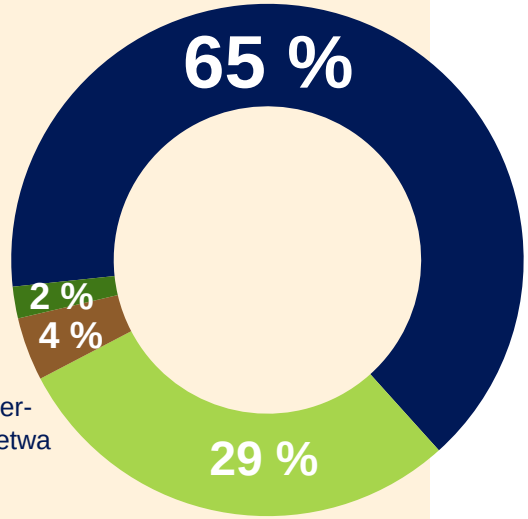
Fast 3 von 4 Unternehmen liegen ohne IT lahm.

Quelle: Forsa-Umfrage „Cyberrisiken im Mittelstand“

„Datenlecks? Uns doch egal!“

Haben Sie geprüft, ob Ihr Unternehmen betroffen ist?

Wissen nicht, ob ihre Daten bereits kursieren



Von denjenigen, die Ihre Daten über-prüft haben, war etwa jeder 6. betroffen

- Habe nicht überprüft
- Habe überprüft, war aber nicht betroffen
- Habe überprüft, war betroffen
- Keine Angaben/Weiß nicht

Quelle: Forsa-Umfrage „Cyberrisiken im Mittelstand“

Sind Sie betroffen? Hier finden Sie es heraus.

Der Service „Have I Been Pwned?“ (Pwned wird gesprochen wie „poned“) hat über 6 Milliarden Datensätze aus mehr als 300 Datenlecke gesammelt. Wenn Sie überprüfen wollen, ob auch Ihre Mail-Adresse darunter ist, geben Sie diese einfach in der entsprechenden Suchmaske ein, das Ergebnis wird sofort angezeigt.

→ https://haveibeenpwned.com/

Das Hasso-Platter-Institut bietet den „HPI Identity Leak Checker“ an. Sie können anhand Ihrer E-Mail-Adresse prüfen, ob die Adresse in Verbindung mit anderen persönlichen Daten wie Geburtsdatum oder Adresse im Internet offengelegt wurde und missbraucht werden könnte. Anders als bei „Have I Been Pwned?“ erhalten Sie das Ergebnis per Mail.

→ https://sec.hpi.de/ilc/

Wie viele Schadprogramme gibt es weltweit?

0___.___.___.___500 Mio.

Wie viele Schadprogramme gibt es weltweit?

0____.____.____._I_.___500 Mio.

In 2022 waren es 356 Mio.

Richtig

Wie viele Schadprogramme kommen täglich hinzu?

0_____500 T.

Wie viele Schadprogramme kommen täglich hinzu?

300 T 400T

0 500 T.

in 2022 waren es 396.000

Richtig

Was ist passiert und *was* können die Folgen eines Cyberangriffes sein?

Eingang einer E-Mail im Postfach des Geschäftsführers, die als Absender das zuständige Arbeitsamt ausweist.

Das Unternehmen sucht in Abstimmung mit dem Arbeitsamt seit längerem qualifizierte Fachkräfte. Eine Kommunikation via E-Mail ist vereinbart und abgesprochen.

Die betreffende E-Mail wurde geöffnet, da der Absender und das Format keine Veranlassung zu Vorsichtsmaßnahmen gibt. Im Anhang der Nachricht befindet sich ein PDF

Beim Öffnen des Anhangs erscheint auf dem Bildschirm eine Sonnenblume, die ein Blütenblatt nach dem anderen fallen lässt.

Aufträge können nicht fertig-gestellt oder bearbeitet werden, da Informationen zum Stand und den Absprachen digital erfasst sind.

Termine ggü. den Auftraggebern können nicht eingehalten werden, da diese digital eingestellt und über-wacht werden.

Die Aktivierung der Backup gestaltet sich als schwierig, denn es liegt eine externe Verschlüsselung auf den Datenpaketen.

„Verloren gegangene Daten“ müssen aufwendig neu erstellt bzw. beim Kunden neu angefordert werden.

PCs müssen ausgetauscht und mit neuer Lizenzsoftware ausgestattet werden.

Es fanden Zugriffe über den Hauptrechner auf Bank-konten statt, die nicht erklärbar waren und in Zusammenhang mit dem Cyberangriff stehen.

Langwierige Gespräche mit den Auftraggebern mit Erläuterung zu dem Vorfall und der Bitte um Verständnis der Terminverschiebung.

Mitarbeiter waren über den Zeitraum von ca. 2 Wochen nur eingeschränkt arbeitsfähig.

Eigenschäden
Betriebsbeeinträchtigung / -unterbrechung

Finanzielle Auswirkungen	
Voller Einsatz des IT-Teams (interne Ressourcen)	13.000 EUR
Mitwirken eines Spezialistenteams (Internetanbieter + Forensik)	18.500 EUR
Massive Beinträchtigung der Handlungsfähigkeit 14 Tage	135.000 EUR
Beeinträchtigung des Images und Beeinträchtigung des Ratings in Foren	18.500 EUR
Verstärkte Marketingaktivität	
Gesamtkosten	**185.000 EUR**

ES IST NICHT DIE FRAGE OB ES PASSIERT, SONDERN WANN…

… EINEN CYBERBRAND KANN MAN NUR SCHWER LÖSCHEN

IT-Sicherheit geht alle an:
Es ist nicht die Frage, ob es passiert, sondern nur, wann

88 %
aller Unternehmen waren in den letzten 2 Jahren von **Diebstahl, Industriespionage oder Sabotage** betroffen. [1]

In **39 %** der Fälle legten Cyberattacken Unternehmen **4 Tage und länger** lahm. [2]

In **86 %** der Fälle verursachen **Cyberangriffe Schäden.** [1]

31 %
Infizierung mit Schadsoftware = häufigste Art von Cyberangriffen. [1]

Ca. **80 %** der Unternehmen haben **Lücken bei der IT-Sicherheit.** [3]

Fatale Fehl-einschätzung
Knapp **3/4 der Unter-nehmen** glaubt: **„Mich wird es nicht treffen."** [2]

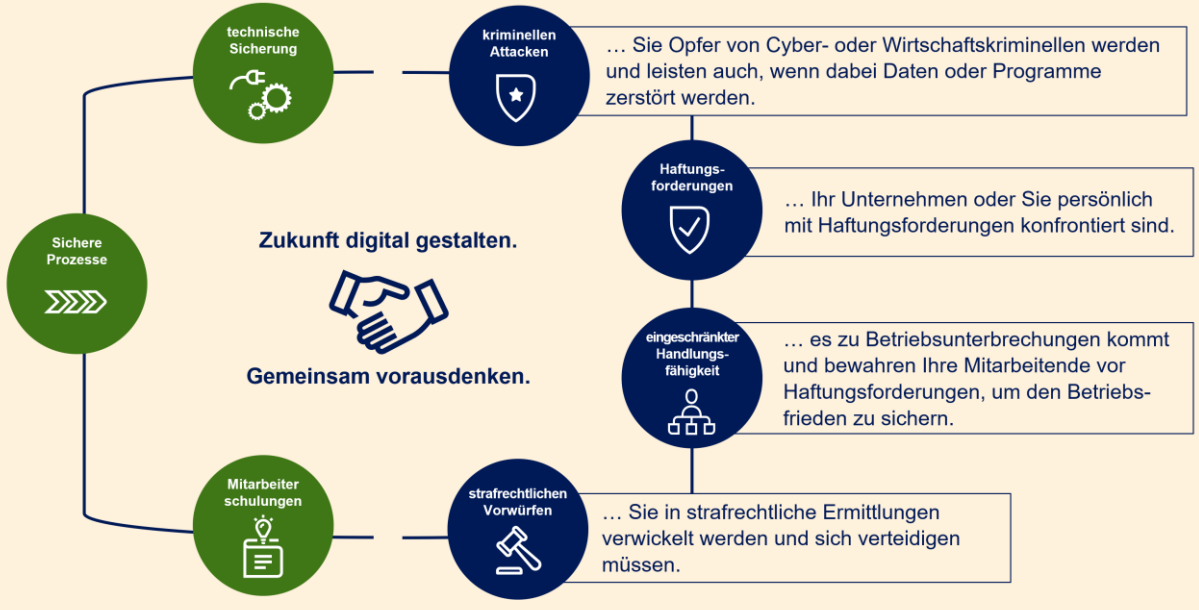
223,5
Milliarden Euro beträgt das Volumen aller Cyberschäden 2021. [1]

[1]Bitkom Research (2021): Wirtschaftsschutz 2021. Berlin. [2]Repräsentative Forsa-Befragung von 300 Entscheidern in kleinen und mittleren Unternehmen im April 2021. [3]Gesamtverband der Deutschen Versicherungswirtschaft e. V.(2021): Report Cyberrisiken im Mittelstand 2021. Berlin.

PARTNERSCHAFT FÜR DEN ERFOLG – LÖSUNGEN FÜR IHRE IT-SICHERHEIT

Sie beugen bereits heute weitsichtig vor.

Wir sorgen darüber hinaus für Ihre finanzielle Absicherung.



Ihre Vorteile auf einen Blick:

- ✓ Umfassender finanzieller Schutz aus einer Hand
- ✓ Handlungsfähigkeit sicherstellen
- ✓ Schutz vor privaten Haftungsrisiken
- ✓ Existenzschutz fürs Unternehmen
- ✓ Schutz gegen die Kostenrisiken eines Rechtsstreits
- ✓ Schnelle Hilfe im Schadensfall: finanziell und Assistance-Leistungen
- ✓ Reputationsschäden vermeiden
- ✓ Mitarbeitende vor Haftungsansprüchen schützen

Stand: XX/202X
R+V Allgemeine Versicherung AG

R+V Du bist nicht allein.

Genossenschaftliche FinanzGruppe
Volksbanken Raiffeisenbanken

Vielen Dank für Ihre Aufmerksamkeit

Du bist nicht allein.