Cyber-Risken für Immobilienverwaltungen

–

Prävention, Haftung und richtiges Vorgehen im Schadenfall

INCON

Ludwig Reindl
Leiter Produkt- und Risikomanagement
ludwig.reindl@incon-vm.de
Mobil: 0151 70 29 11 54

VDIV-INCON
2011 bis 2021

Versicherer
Produktmanager
2022 bis 2024

VDIV-INCON
Seit 01.01.2024

Produkt- und Risikomanagement

- Versicherer
- Rahmenverträge
- Firmenversicherungen
  Baumaßnahmen
  Gewerbeimmobilien
- Wissensvermittlung

INCON

AGENDA

1) Die Entwicklung von Cyberangriffen
2) Reale Cyberangriffe aus der Praxis
3) Wenn Daten plötzlich weg sind
4) Haftungsrisiken für Immobilienverwaltungen
5) Cyber-Versicherung als Schutzbaustein
6) Woran man eine gute Cyber-Risk-Versicherung erkennt

INCON

Die Entwicklung von Cyberangriffen

Wie sich digitale Bedrohungen in den letzten zehn Jahren verändert haben

–

und warum Immobilienverwaltungen heute stärker betroffen sind

INCON

Die Entwicklung von Cyberangriffen

1. Wandel der Cyberangriffe (ca. 2015 → 2025)

- Cyberkriminalität hat stark zugenommen und erreicht regelmäßig neue Höchststände – 2025:
  - 289,2 Milliarden € + Dunkelziffer
  - 1.220 Cyberangriffe pro Woche pro Unternehmen (=175 pro Tag)
  - 87% der Unternehmen betroffen
- Cyberangriffe sind **professioneller und organisierter**
  - Täter nutzen automatisierte Tools/Dienstleistungen („Cybercrime-as-a-Service“)
  - Täter agieren international, anonymisiert und mit hoher technischer Expertise
- Angriffe zielen zunehmend auf **leicht angreifbare, aber lukrative Branchen**

„Hacker“
als Einzelakteure

Cybercrime-Ökosysteme
(Banden, Dienstleister, staatliche Gruppen)

INCON

2. Warum Immobilienverwaltungen heute stärker betroffen sind

Große Mengen sensibler Daten

Immobilienverwaltungen verarbeiten:

- personenbezogene Daten (Mieter, Eigentümer)
- Bankverbindungen
- Mietverträge und Abrechnungen

👉 **für Angreifer extrem wertvoll!**
(Identitätsdiebstahl, Betrug)

INCON

2. Warum Immobilienverwaltungen heute stärker betroffen sind

Finanzielle Transaktionen als Angriffsziel

Ein besonders wichtiger Punkt:

- Regelmäßige Überweisungen (Miete, Nebenkosten, Kautionen)
- Hohe Geldsummen im Umlauf

Typischer Angriff:

👉 **Manipulation von Zahlungsdaten** (z. B. gefälschte E-Mails mit neuer Kontoverbindung)

Das ist eine Form von **Social Engineering** – und heute eine der erfolgreichsten Methoden.

INCON

2. Warum Immobilienverwaltungen heute stärker betroffen sind

Geringere IT-Sicherheitsstandards

Viele Immobilienverwaltungen:

- sind mittelständisch
- haben begrenzte IT-Budgets
- nutzen veraltete Software oder schlecht gesicherte Systeme

👉 Im Vergleich zu Banken oder Konzernen sind sie oft **leichter angreifbar**

2. Warum Immobilienverwaltungen heute stärker betroffen sind

Zunehmende Digitalisierung der Branche

In den letzten Jahren:

- digitale Eigentümer- und Mieterportale
- Cloud-Lösungen
- Online-Dokumentenverwaltung

👉 **Mehr digitale Prozesse = mehr Angriffsfläche**

INCON

2. Warum Immobilienverwaltungen heute stärker betroffen sind

Vertrauensbasierte Kommunikation

Ein entscheidender Schwachpunkt:

- Kommunikation läuft oft per E-Mail
- Eigentümer vertrauen Anweisungen ihrer Verwaltung

👉 **Angreifer nutzen genau dieses Vertrauen aus**
(z. B. gefälschte Rechnungen)

INCON

Die Entwicklung von Cyberangriffen

3. Typische Angriffe auf Immobilienverwaltungen

1. Phishing & CEO-Fraud

- Gefälschte E-Mails im Namen der Verwaltung
- Ziel: Geldüberweisungen umleiten

👉 Besonders gefährlich, weil schwer zu erkennen

2. Ransomware

- Systeme werden verschlüsselt
- Zugriff auf Daten und Dokumente blockiert

👉 Kann den gesamten Betrieb lahmlegen

3. Datenlecks

- Diebstahl von Eigentümer-, Mieter- und Vertragsdaten
- Veröffentlichung oder Verkauf im Darknet

👉 Haftung für Drittschaden / Eigenkosten für Reputationsschaden

4. Konto- und E-Mail-Hacking

- Übernahme von E-Mail-Konten
- Versand glaubwürdiger Betrugsnachrichten

👉 Identitätsdiebstahl führt zu finanziellen Schäden

INCON

4. Warum die Bedrohung zunimmt

Die Kombination ist entscheidend:

- **hoher finanzieller Nutzen für Angreifer**
- **vergleichsweise schwache Sicherheitsstrukturen**
- **stark gewachsene Digitalisierung**
- **menschlicher Faktor (Vertrauen, Routine)**

👉 **Immobilienverwaltungen sind damit ein klassisches „lohnendes Ziel mit niedriger Eintrittshürde“.**

INCON

5. Fazit

In den letzten zehn Jahren hat sich die Bedrohungslage stark verändert:

- Angriffe sind gezielter und **raffinierter** geworden
- Der Fokus verschiebt sich auf Branchen wie Immobilienverwaltungen
- Besonders **Betrug über Kommunikation (E-Mail, Zahlungsänderungen)** steht im Vordergrund

👉 Immobilienverwaltungen sind heute nicht mehr „Randziel“, sondern ein **bewusst ausgewähltes Angriffsziel**, weil sie Geld, Daten und Vertrauen kombinieren.

INCON

Reale Cyberangriffe aus der Praxis

Aktuelle Beispiele aus der Wirtschaft und dem Verwaltungsalltag.

INCON

Reale Cyberangriffe aus der Praxis

✈️ Angriff auf Flughafen-Systeme (09/2025)

- Ziel: IT-Dienstleister von Flughäfen (u. a. Berlin BER)
- Art: **Ransomware-Angriff** (Verschlüsselung von Daten um Lösegeld zu fordern)
- Folgen:
  - Check-in- und Gepäcksysteme gestört oder ausgefallen
  - Verspätungen/Ausfälle der Flüge

👉 Ein externer Dienstleister wurde gehackt, wodurch gleich mehrere Flughäfen betroffen waren.

Lerneffekt:
Angriffe treffen oft nicht direkt das Unternehmen, sondern **Zulieferer oder Dienstleister**.

INCON

Reale Cyberangriffe aus der Praxis

Personenbezogene Daten abgeflossen - Cyberangriff trifft Wohnungsgesellschaft in Senftenberg (09/2025)

- Ziel: kommunale Wohnungsgesellschaft
- Art: **Ransomware**
- Folgen:
  - IT-Systeme verschlüsselt
  - Kommunikation (E-Mail, Telefon) gestört
  - Abfluss von personenbezogenen Daten

👉 Betrieb nur noch eingeschränkt möglich.

Lerneffekt:

Immobilienverwaltungen sind ein **konkretes Angriffsziel**.

INCON

Reale Cyberangriffe aus der Praxis

Phishing-E-Mail Anhang geöffnet

Ziel: Immobilienverwaltung

- Zugriff auf E-Mail-Konto durch Phishing
- Mitlesen laufender Kommunikation
- Manipulation einer Zahlungsanweisung
- Überweisung auf Täterkonto

Folgen für die Verwaltung

- finanzieller Schaden durch Fehlüberweisung
- Vertrauensverlust bei Eigentümern
- hoher interner Prüf- und Aufklärungsaufwand
- DSGVO-Meldung bei Datenzugriff

INCON

Wenn Daten plötzlich weg sind

Was Datenverlust für Ihre Verwaltung bedeutet – und wie Sie es verhindern.

INCON

Wenn Daten plötzlich weg sind

Was bedeutet Datenverlust für die Immobilienverwaltung?

- Verlust von **Vertragsdaten, Abrechnungen und Dokumenten**
- Fehlende **Mieter- und Eigentümerdaten**
- Unterbrechung von **Buchhaltung und Zahlungsprozessen**
- Risiko von **rechtlichen Konsequenzen** (z. B. Nachweispflichten)
- **Vertrauensverlust** bei Kunden und Partnern

👉 **Ergebnis: Betrieb kann teilweise oder vollständig stillstehen**

INCON

Wenn Daten plötzlich weg sind

Mögliche Folgen im Alltag

- Nebenkostenabrechnungen nicht mehr nachvollziehbar
- Offene Forderungen gehen verloren
- Kommunikationshistorien fehlen
- Verzögerungen bei Vermietung und Verwaltung
- Hoher manueller Aufwand zur Wiederherstellung

👉 **Zeitverlust + finanzielle Schäden**

INCON

Wenn Daten plötzlich weg sind

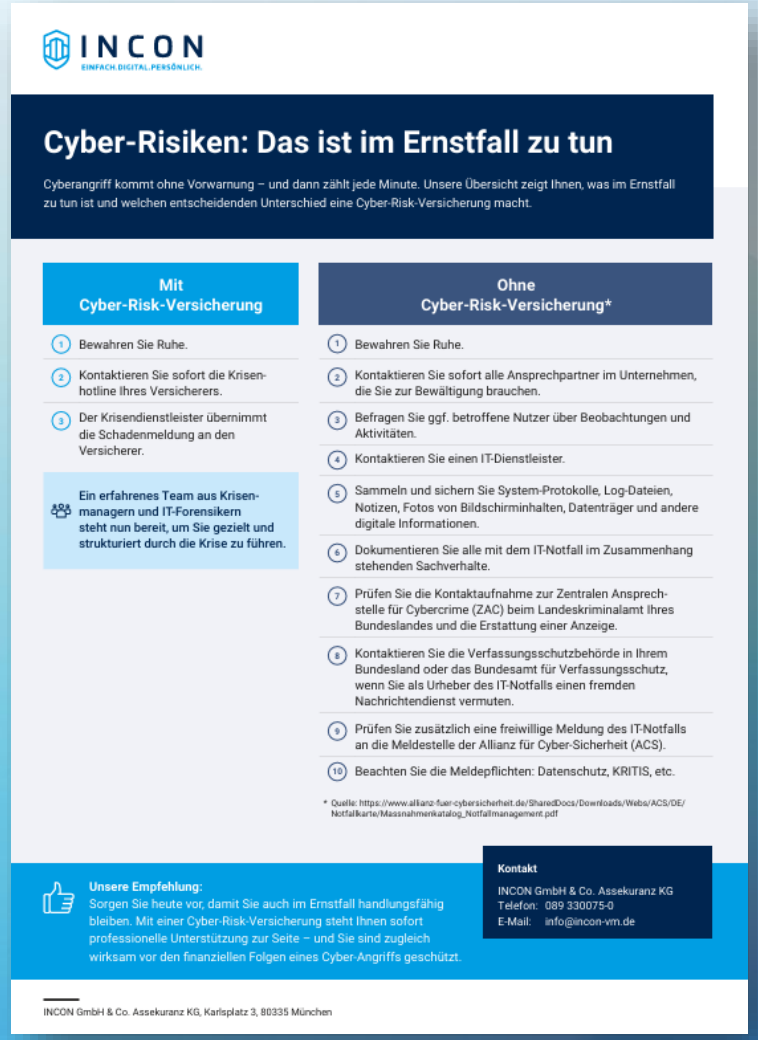
Wie kann man Datenverlust verhindern?

- **Regelmäßige Backups** (automatisiert, täglich)
- Nutzung der **3-2-1-Regel**
- Einsatz von **Cloud-Lösungen**
- Klare **Zugriffsrechte und Rollenverteilung**
- **IT-Sicherheitsmaßnahmen** (Updates, Virenschutz)
- **Mitarbeiterschulungen**

INCON

Wenn Daten plötzlich weg sind

Vorbereitung auf den Ernstfall



INCON
EINFACH. DIGITAL. PERSÖNLICH.

Cyber-Risiken: Das ist im Ernstfall zu tun

Cyberangriff kommt ohne Vorwarnung – und dann zählt jede Minute. Unsere Übersicht zeigt Ihnen, was im Ernstfall zu tun ist und welchen entscheidenden Unterschied eine Cyber-Risk-Versicherung macht.

Mit Cyber-Risk-Versicherung	Ohne Cyber-Risk-Versicherung*
1 Bewahren Sie Ruhe.	1 Bewahren Sie Ruhe.
2 Kontaktieren Sie sofort die Krisen-hotline Ihres Versicherers.	2 Kontaktieren Sie sofort alle Ansprechpartner im Unternehmen, die Sie zur Bewältigung brauchen.
3 Der Krisendienstleister übernimmt die Schadenmeldung an den Versicherer.	3 Befragen Sie ggf. betroffene Nutzer über Beobachtungen und Aktivitäten.
Ein erfahrenes Team aus Krisen-managern und IT-Forensikern steht nun bereit, um Sie gezielt und strukturiert durch die Krise zu führen.	4 Kontaktieren Sie einen IT-Dienstleister.
	5 Sammeln und sichern Sie System-Protokolle, Log-Dateien, Notizen, Fotos von Bildschirminhalten, Datenträger und andere digitale Informationen.
	6 Dokumentieren Sie alle mit dem IT-Notfall im Zusammenhang stehenden Sachverhalte.
	7 Prüfen Sie die Kontaktaufnahme zur Zentralen Ansprech-stelle für Cybercrime (ZAC) beim Landeskriminalamt Ihres Bundeslandes und die Erstattung einer Anzeige.
	8 Kontaktieren Sie die Verfassungsschutzbehörde in Ihrem Bundesland oder das Bundesamt für Verfassungsschutz, wenn Sie als Urheber des IT-Notfalls einen fremden Nachrichtendienst vermuten.
	9 Prüfen Sie zusätzlich eine freiwillige Meldung des IT-Notfalls an die Meldestelle der Allianz für Cyber-Sicherheit (ACS).
	10 Beachten Sie die Meldepflichten: Datenschutz, KRITIS, etc.

* Quelle: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/Notfallkarte/Massnahmenkatalog_Notfallmanagement.pdf

Unsere Empfehlung:
Sorgen Sie heute vor, damit Sie auch im Ernstfall handlungsfähig bleiben. Mit einer Cyber-Risk-Versicherung steht Ihnen sofort professionelle Unterstützung zur Seite – und Sie sind zugleich wirksam vor den finanziellen Folgen eines Cyber-Angriffs geschützt.

Kontakt
INCON GmbH & Co. Assekuranz KG
Telefon: 089 330075-0
E-Mail: info@incon-vm.de

INCON GmbH & Co. Assekuranz KG, Karlsplatz 3, 80335 München

- Notfallplan (Disaster Recovery) definieren
- Zuständigkeiten klar festlegen
- Wiederherstellung regelmäßig testen
- Schnelle Reaktionsfähigkeit sicherstellen

👉 dok.incon-it.de/download.php?alias=Checkliste-Cyberrisk

INCON

Haftungsrisiken für Verwalter

Welche rechtlichen Folgen Cyberangriffe haben – und gegenüber wem Verwalter haften

INCON

Haftungsrisiken für Verwalter

Haftungsrisiken durch Cyberangriffe

- Cyberangriffe (z. B. Ransomware, Datenlecks) können zu **Datenverlust und Datenmissbrauch** führen
- Immobilienverwaltungen verarbeiten **sensible personenbezogene Daten** (Mieter, Eigentümer, Kontodaten)
- Gesetzliche Pflicht zur **Datensicherheit und -verfügbarkeit**

👉 Cyberangriffe sind nicht nur IT-Probleme, sondern **rechtliche Risiken**

INCON

Haftungsrisiken für Verwalter

Rechtliche Folgen eines Cyberangriffs

- **Schadensersatzansprüche** von Betroffenen (z. B. Mieter, Eigentümer)
- **Bußgelder** wegen Verstößen gegen Datenschutzvorgaben (z. B. DSGVO)
- **Vertragsverletzungen** gegenüber Eigentümern/Auftraggebern
- **Meldepflichten** bei Datenschutzverletzungen (innerhalb von 72 Stunden)
- Reputationsschäden und Vertrauensverlust

INCON

Haftungsrisiko

Benachrichtigung, Art. 33 DSGVO:
Wenn ein Datenschutzvorfall zu einem Risiko für die **Rechte und Freiheiten** von natürlichen Personen führen **kann**, muss der Vorfall innerhalb von **72 Stunden** an die Behörden gemeldet werden.

Nichtbefolgung kann teuer werden!

Bußgelder
Gem. Art. 83 DSGVO können **Bußgelder bis 20 Mio. € oder 4% Umsatzes** verhängt werden.

Verantwortlich
Verantwortlich ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt.

Haftung
Vorstände, Geschäftsführer oder für den IT-Bereich Verantwortliche, also alle, die allein oder gemeinsam mit anderen **über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden**, sind Verantwortliche **gem. Art. 26 DSGVO**.

INCON

Haftungsrisiken für Verwalter

Wem gegenüber haftet die Immobilienverwaltung?

1. Eigentümer / Auftraggeber
- Verletzung des Verwaltervertrags
- z. B. bei Datenverlust, finanziellen Schäden oder Organisationsversagen

2. Eigentümer/Mieter
- Schutz personenbezogener Daten
- Haftung bei Datenlecks oder Missbrauch

3. Behörden
- Einhaltung von Datenschutzgesetzen
- mögliche Bußgelder bei Verstößen

4. Geschäftspartner / Dienstleister
- z. B. bei weitergegebenen oder kompromittierten Daten

INCON

Haftungsrisiken für Verwalter

Typische Haftungsszenarien

- Hackerangriff → Kontodaten von Eigentümern/Mietern werden gestohlen
- Fehlendes Backup → wichtige Abrechnungen gehen verloren
- Phishing-Mail → falsche Überweisung ausgelöst
- Unzureichende IT-Sicherheit → DSGVO-Verstoß

👉 **Oft Kombination aus technischem und organisatorischem Versagen**

INCON

Haftungsrisiken für Verwalter

Wie kann Haftung reduziert werden?

- Technische Schutzmaßnahmen (Firewalls, Updates, Zugriffsschutz)
- Regelmäßige Datensicherungen
- Dokumentierte Prozesse und IT-Richtlinien
- Schulung der Mitarbeiter (Phishing, IT-Sicherheit)
- Sorgfältige Auswahl von IT-Dienstleistern
- **Abschluss einer Cyber-Versicherung**

INCON

Cyber-Versicherung als Schutzbaustein

Welche Leistungen im Ernstfall wirklich helfen.

INCON

Cyber-Versicherung als Schutzbaustein

Soforthilfe im Ernstfall

- IT-Forensik zur Ursachenanalyse
- Unterstützung bei Systemwiederherstellung
- Krisenmanagement und Notfall-Hotline
- Kommunikation mit Behörden und Betroffenen

👉 **Schnelle Reaktion reduziert Schaden erheblich**

INCON

Cyber-Versicherung als Schutzbaustein

Übernahme von Kosten

- Wiederherstellung von Daten und Systemen
- **Betriebsunterbrechung (entgangene Einnahmen)**
- IT-Dienstleister und externe Spezialisten
- Kosten für Benachrichtigung Betroffener

👉 **Fokus: finanzielle Entlastung**

INCON

Cyber-Versicherung als Schutzbaustein

Absicherung von Haftungsrisiken

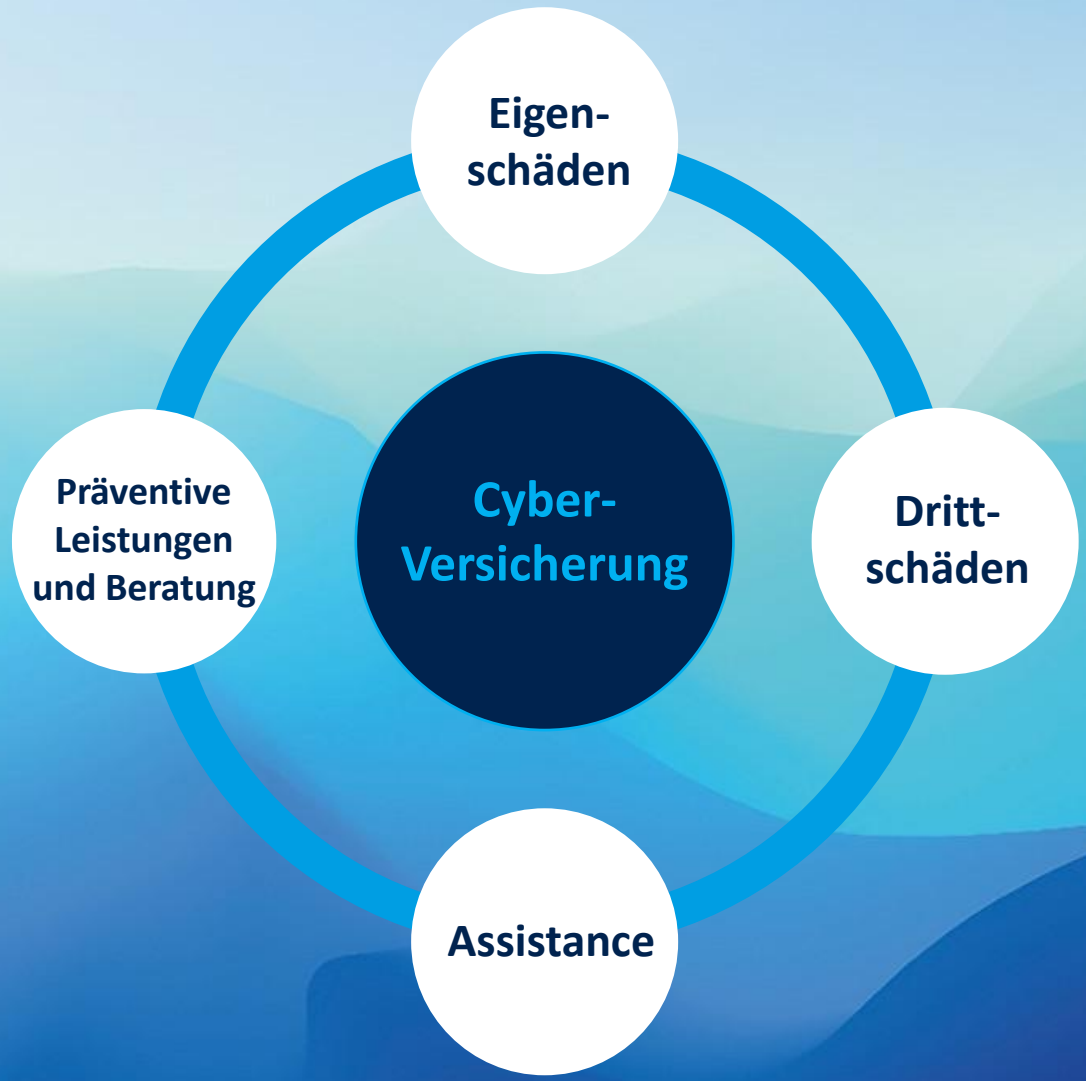
- Prüfung von Schadensersatzansprüchen
- Übernahme berechtigter Forderungen
- Abwehr unberechtigter Ansprüche (Rechtsschutz)
- Unterstützung bei Datenschutzverstößen

👉 **Schutz gegenüber Dritten (Mieter, Eigentümer,etc.)**

INCON

Cyber-Versicherung als Schutzbaustein

Absicherung vor Cyber-Risiken - die Cyber-Versicherung



INCON

Woran man eine gute Cyber-Versicherung erkennt

Entscheidende Qualitätsmerkmale, die im Schadenfall den Unterschied machen.

INCON

Richtig oder Mythos?

Regelt mein IT Dienstleister

100.000 € bereits versichert

„Beruhigungsvertrag“

INCON

Woran man eine gute Cyber-Versicherung erkennt

Ermittlung der Versicherungssumme

- Anzahl der verwalteten Einheiten
- Jahresumsatz
- Grad der Digitalisierung (je höher, desto angreifbarer)
- Betriebsunterbrechung berücksichtigen
- Haftungsrisiken nicht unterschätzen
- Lieber zu hoch als zu niedrig versichern

INCON

Woran man eine gute Cyber-Versicherung erkennt

Beispiel Versicherungssumme bei 2.500 WE

1. IT-Forensik & Wiederherstellung - Eigenschaden

ca. 85.000 – 150.000 €

2. Betriebsunterbrechung (laufende Personalkosten + entgangene Einnahmen)

ca. 15.000 – 30.000 €

3. Haftungsrisiken – Schadensersatzforderungen Dritter

ca. 200.000 – 300.000 €

4. DSGVO-Bußgelder & rechtliche Kosten

ca. 50.000 – 200.000 €

5. Krisenmanagement & Kommunikation

ca. 30.000 – 80.000 €

Gesamtschaden zwischen 380.000 € bis 760.000 €!

INCON

Woran man eine gute Cyber-Versicherung erkennt

Antragsfragen und Obliegenheiten

- Vollständige wöchentliche Datensicherung
- Aufbewahrung der vollständigen Datensicherung über mind. 30 Tage
- Nutzung einer Offline-Datensicherung mit dauerhafter physischer Trennung von den IT-Systemen ODER Nutzung einer unveränderbaren Online-Datensicherung, auf welche die Administratoren nur mit einer von der betreffenden Domäne unabhängigen Zwei-Faktor-Authentifizierung oder aus einer separaten Domäne zugreifen können.
- Updates innerhalb von 30 Tagen nach Veröffentlichung
- Keine Betriebssysteme, für die keine Updates gestellt werden

INCON

Woran man eine gute Cyber-Versicherung erkennt

Fehlende Deckungsinhalte

- Nicht nur Kosten zahlen, sondern **Aktive Krisenbegleitung**
- Keine oder eingeschränkte Betriebsunterbrechung
- Deckung bei menschlichen Fehlern
  (Bedien- und Programmierfehler)
- Cyber-Erpressung (Lösegeld)
- Cyber-Betrug (Fake-President)
- Stand der Technik-Falle
- KI-Ausschluss

INCON

Kurz gesagt

Die Frage ist nicht OB eine Cyber-Attacke eintritt, sondern WANN!

Eine Cyberversicherung ersetzt nicht den Schutz vor einer Cyberattacke.

Eine Cyberversicherung hilft, die Folgen eines Angriffs zu bewältigen.

INCON

Was nun?

INCON

Für eine Beratung stehe ich Ihnen gerne zur Verfügung!

ludwig.reindl@incon-vm.de