Stefan Leber

Online Seminar

Cyberriskversicherung und Wirtschaftskriminalität in der UnternehmensPolice (UNP)

KRAVAG R+V CONDOR

Die R+V Versicherungsgruppe

Stefan Leber

Produktförderer MultiLine

KRAVAG R+V CONDOR

Die R+V Versicherungsgruppe

Agenda Cyberrisk und Wirtschaftskriminalität

1. Bedrohungslage
2. Kundenansprache
3. Übersicht
4. Highlights
5. R+V UnternehmensPolice (UNP)
6. Selbsttest

https://www.sicherheitstacho.eu/start/main

Bedrohungslage: Der Angriff kommt

Nicht „ob“, sondern nur „wann“ ist die Frage

Über das Projekt

Das Honeypot-Projekt der Deutschen Telekom erzeugt absichtlich verlockende Ziele, die für potenzielle Angreifer attraktiv erscheinen, aber keinerlei echte Informationen preisgeben. Sobald ein Angreifer auf diese Köder hereinfällt und versucht, unsere vermeintlichen Schwachstellen auszunutzen, zeichnen wir ihre Aktivitäten auf. Auf diese Weise erhalten wir wertvolle Erkenntnisse über Angriffsmuster und können unsere realen Systeme effektiv schützen.

KRAVAG R+V CONDOR

Wer soll uns denn schon hacken?

Über 86% der erfolgreichen Angriffe gelingen über die Mitarbeiter.

In der Regel handeln die Mitarbeiter ohne böse Absicht oder kriminelle Energie. Oft sind es Zufallstreffer.

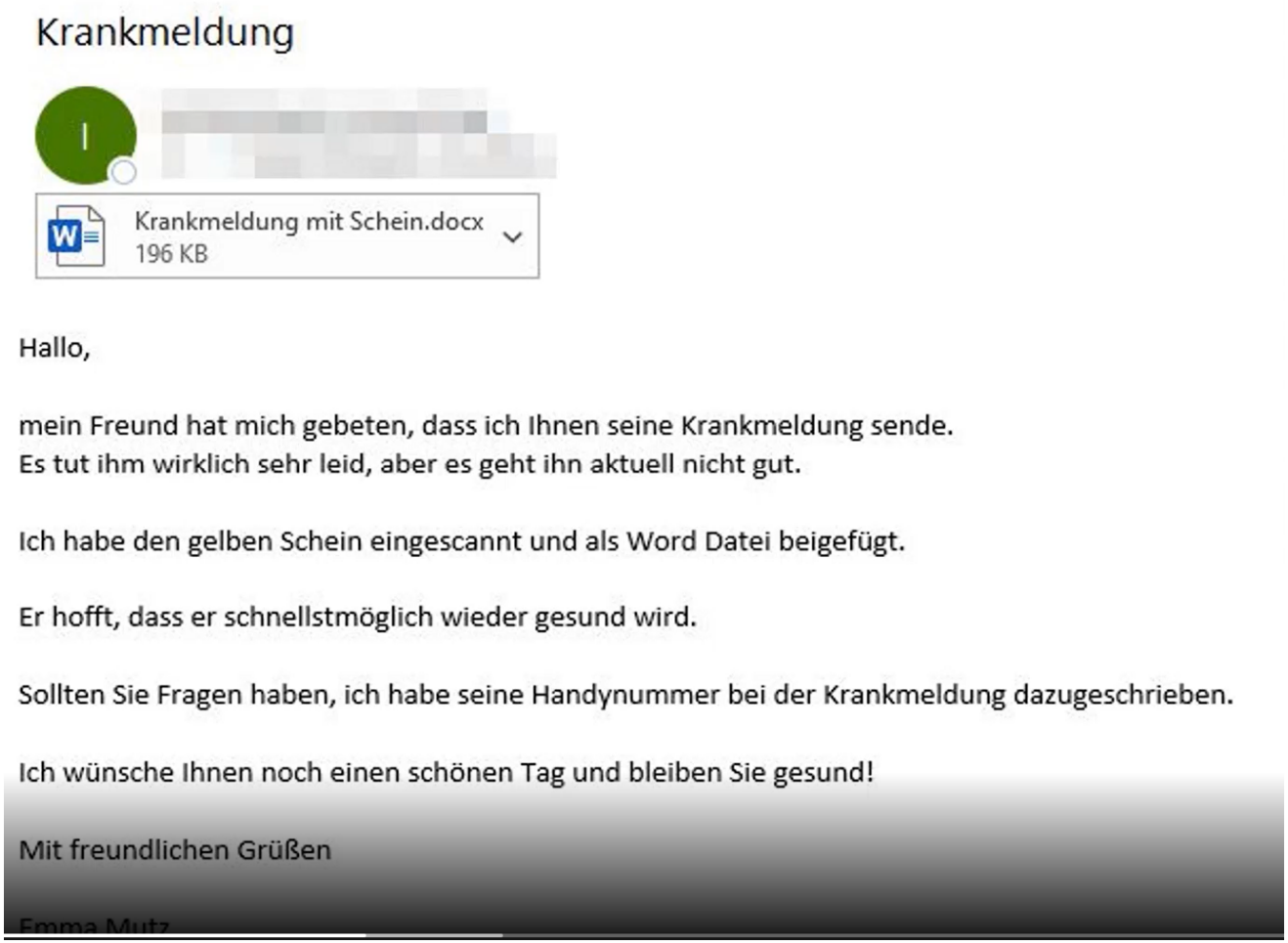
Wer soll uns denn schon hacken?

Über 86% der erfolgreichen Angriffe gelingen über die Mitarbeiter.

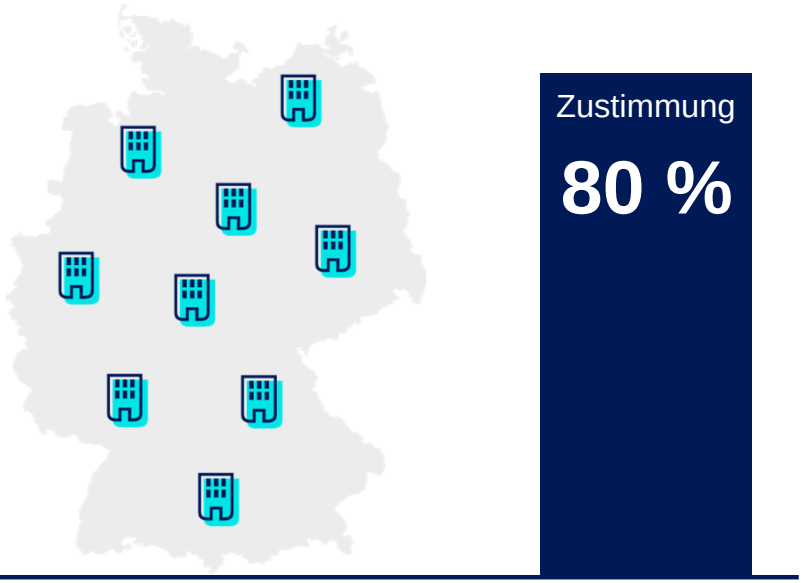
In der Regel handeln die Mitarbeiter ohne böse Absicht oder kriminelle Energie. Oft sind es Zufallstreffer.

KRAVAG R+V CONDOR

Der Mensch wird „gehackt“



Umfrage 2023: „Das Risiko gibt es, aber mein Unternehemen betrifft es nicht“



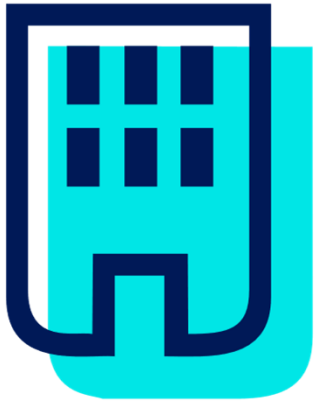
Zustimmung

80 %

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
Grafik: www.gdv.de I Gesamtverband der Deutschen Versicherungswirtschaft (GDV)

KRAVAG R+V CONDOR

Kunden erfolgreich überzeugen

Sie schildern einem Kunden das folgende Szenario:

„Der Geschäftsführer eines mittelständischen Betriebes wird am frühen Montagmorgen um 6:00 Uhr durch einen Anruf seines Büroleiters geweckt.
Im Betrieb sind alle Bildschirme „schwarz“,
der Zugriff auf die Systeme und Daten ist nicht mehr möglich.
Telefon und Fax sind „tot“.
Klar erkennbar – die IT wurde erfolgreich angegriffen / gehackt.“

Was würden Sie jetzt tun?

KRAVAG R+V CONDOR

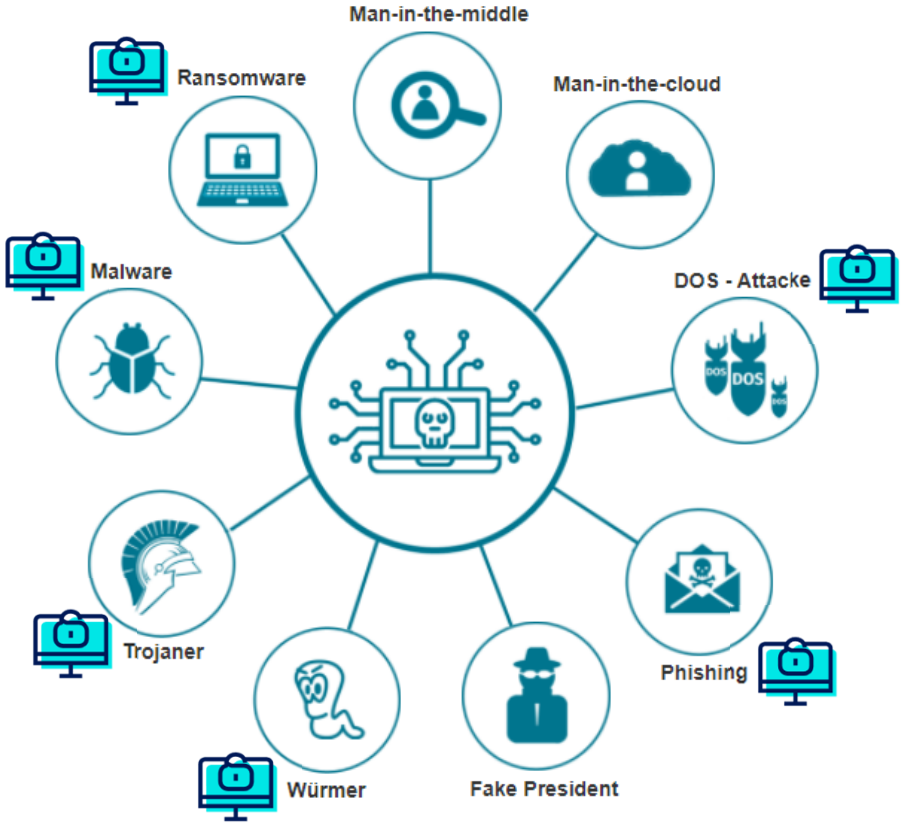
Ihr Kunde – in trügerischer Sicherheit

1. Fragen Sie Ihren Kunden, was für ihn in dieser Situation am allerwichtigsten ist.

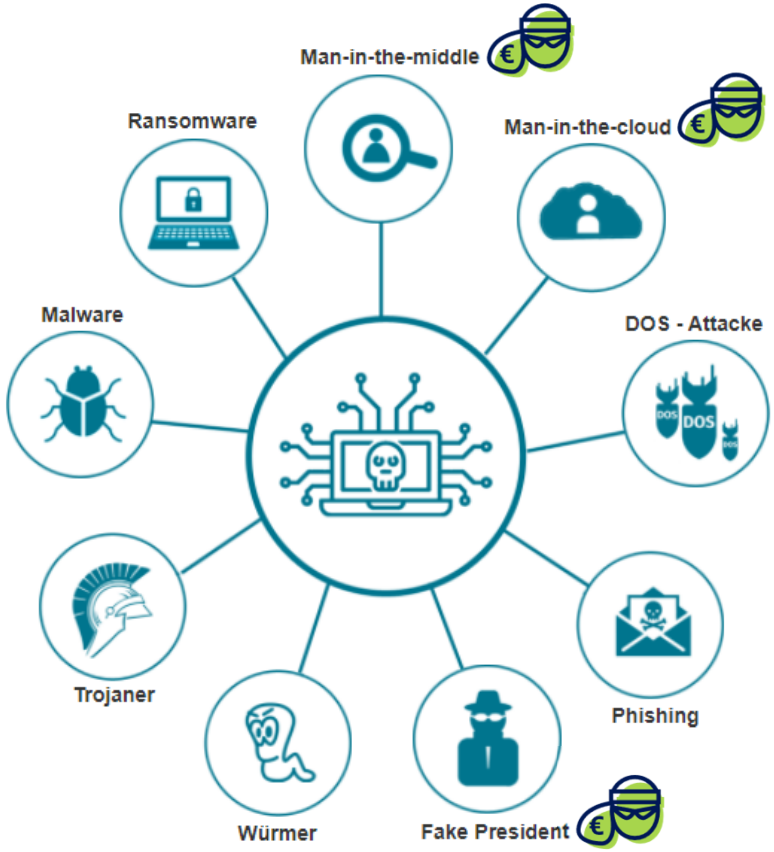
2. Begegnen Sie möglichen Einwänden wie
   - „Wir sind noch nie gehackt worden“
   - „Wer sollte uns denn schon hacken?“
   - „Ich habe einen guten IT-Spezialisten“
   - „Wir arbeiten mit DATEV und sind bestens geschützt“
   - „Die interne IT hat gar keine Internet-Anbindung“

CyberRisk + Wirtschaftskriminalität MultiLine

Cyberkriminalität:



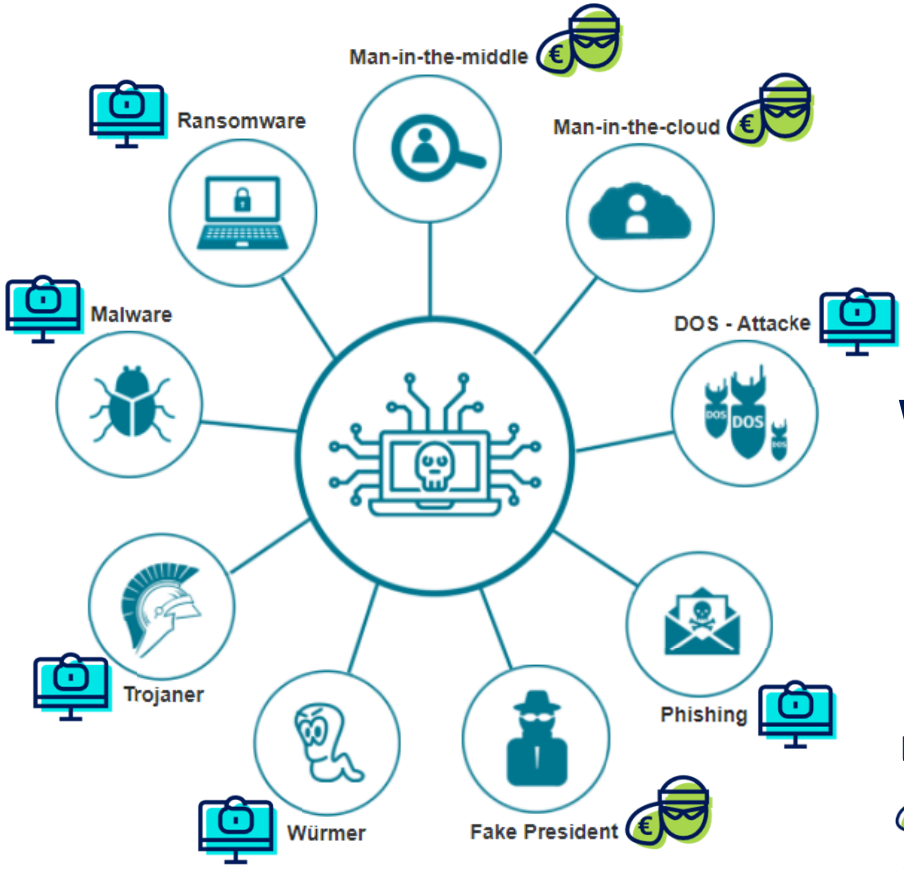
CyberRisk + Wirtschaftskriminalität MultiLine



Wirtschaftskriminalität:

CyberRisk + Wirtschaftskriminalität MultiLine

Cyberkriminalität:



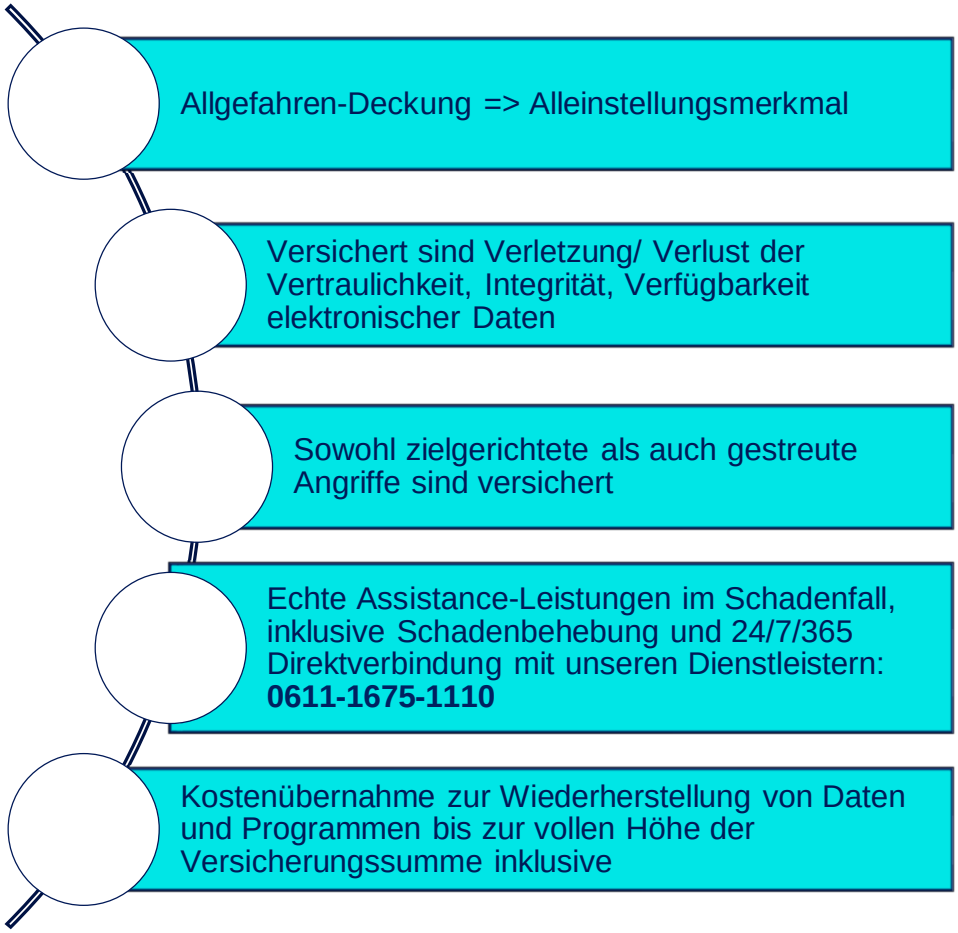
Wirtschaftskriminalität:

Hierzu zählen unter anderem auch:

- Diebstahl
- Unterschlagung und Untreue
- durch Vertrauenspersonen
- durch eigene Mitarbeiter

KRAVAG R+V CONDOR

Highlights CyberRisk



Highlights CyberRisk und Wirtschaftskriminalität

- Allgefahren-Deckung => Alleinstellungsmerkmal
- Versichert sind Verletzung/ Verlust der Vertraulichkeit, Integrität, Verfügbarkeit elektronischer Daten
- Sowohl zielgerichtete als auch gestreute Angriffe sind versichert
- Echte Assistance-Leistungen im Schadenfall, inklusive Schadenbehebung und 24/7/365 Direktverbindung mit unseren Dienstleistern: **0611-1675-1110**
- Kostenübernahme zur Wiederherstellung von Daten und Programmen bis zur vollen Höhe der Versicherungssumme inklusive

- Betriebsunterbrechung bis zur vollen Höhe der Versicherungssumme inklusive.
  Nur 6 Stunden Selbstbeteiligung.
- Ersatz von dienstlichen und privaten Daten auf dienstlich genutzten Privatgeräten (BYOD)
- Beispiele für versicherte Betrugsszenarien durch Dritte: Bestellbetrug, Lieferbetrug, Überweisungsbetrug, CEO-Fraud
- Wissentliche Pflichtverletzung durch Vertrauenspersonen, inklusive Geheimnisverrat und Betriebsspionage
- Kosten für Vertragsstrafen, Betriebsunterbrechung, Wiederherstellung von Daten

KRAVAG R+V CONDOR

Produktdetails CyberRisk (MultiLine)

Die CyberRisk Versicherung bietet Unternehmen bis 25 Mio. EUR Umsatz eine umfassende Absicherung für die Gefahren, die aus der Nutzung von elektronischen Daten auf Informations- und Telekommunikationsgeräten entstehen. Gegenstand der Versicherung ist die Verletzung der Vertraulichkeit, Integrität sowie Verfügbarkeit von Daten.

- Ersetzt werden Eigen- und Drittschäden sowie Kosten.
- Versichert sind Sach- und Vermögensschäden.
- Versicherungsschutz für Personenschäden und erweiterte Sachschäden ist optional erhältlich.
- Die CyberRisk Versicherung ist eine **Allgefahrendeckung.**

Versicherungssummen:	25.000 EUR, 50.000 EUR, 100.000 EUR, 250.000 EUR, 500.000 EUR oder sogar 1.000.000 EUR (1-fache Jahresmaximierung)
Selbstbeteiligung:	150 EUR, 250 EUR, 500 EUR, 1.000 EUR, 2.500 EUR oder 5.000 EUR (abhängig von der gewählten Versicherungssumme)
Laufzeit:	ein oder drei Jahre (mit automatischer Verlängerung)

KRAVAG R+V CONDOR

Diese Betriebsarten werden nicht versichert

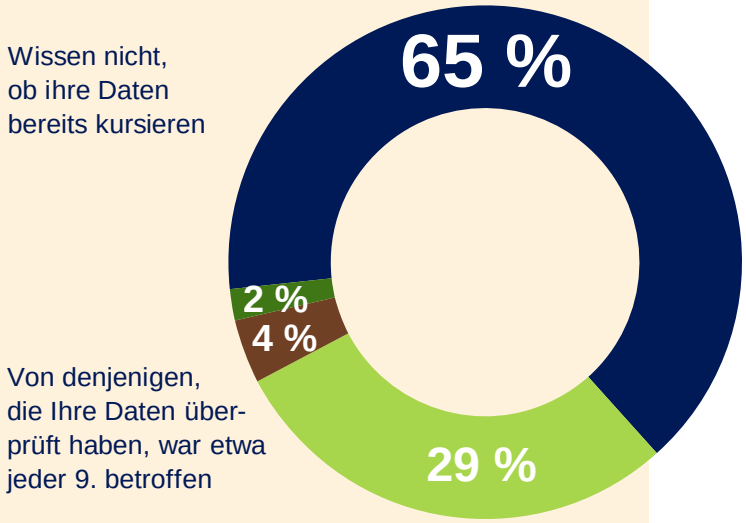
- Krankenhäuser
- IT-Unternehmen (NEU: Bis 100.000 EUR Versicherungssumme möglich)
- Büro eines Dienstleisters (Verein, Verwaltung), Betriebsbeschreibung zu allgemein.
- Ver- und Entsorgungsbetriebe
- Lotterieannahmestellen
- Banken, Kreditinstitute
- Rundfunk- und Fernsehsender

Nur 4 Risikofragen in R+V CONNECT

Risikofrage	Antwort
Betreiben Sie ein Lizenzmanagement für Ihre Standard-Software? (Führen Sie alle angebotenen Updates der Softwarehersteller unverzüglich nach dem Erscheinen aus und haben Sie nur Software im Einsatz, für die Sie eine Lizenz besitzen?)	Offen
Betreiben Sie ein Backup-Management? (Sichern Sie Ihre Daten einschließlich der Software wöchentlich und lagern die Sicherung räumlich und technisch getrennt von Ihrer IT? Prüfen Sie außerdem quartalweise die Qualität der gesicherten Daten? (funktionierendes Backup))	Offen
Haben Sie eine Virensoftware sowie eine Firewall im Einsatz? (Die Virensoftware muss automatisch aktualisiert werden.)	Offen
Haben bei Ihnen im Unternehmen nur IT-Administratoren Administratorenrechte und werden diese ausschließlich für Tätigkeiten als Administrator eingesetzt? (Für die normale tägliche Arbeit dürfen keine Administratorenrechte verwendet werden.)	Offen

„Datenlecks? Uns doch egal!“

Haben Sie geprüft, ob Ihr Unternehmen im Januar 2021 betroffen war?



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/

KRAVAG RHV CONDOR