



Keine Sorgen IT-Sicherheitspaket
Zuverlässiger Schutz für Ihr
Unternehmen in der digitalen Welt

Oberösterreichische
makler.keinesorgen.at

Oberösterreichische
makler.keinesorgen.at

Keine Sorgen
MaklerService
makler.keinesorgen.at

Oberösterreichische
www.keinesorgen.at

Manche Gäste pingen dich

Warum eine Absicherung wichtig ist

Die Digitalisierung und der Einsatz neuer Technologien sind heutzutage nicht mehr aus dem Geschäftsalltag wegzudenken. Mit der zunehmenden Vernetzung steigt jedoch die Gefahr, Opfer eines Cyber-Angriffes zu werden. Von 2004 bis 2017 stieg die Anzahl angezeigter Cyber-Crime-Fälle österreichweit von 754 auf 16.804 an – 2.180 davon alleine in Oberösterreich.

Es geht so schnell – KMUs besonders stark betroffen

Dass kleine und mittlere Unternehmen (KMUs) von IT-Angriffen verschont bleiben, ist falsch. Fast jedes zweite kleine und mittlere Unternehmen war in den letzten beiden Jahren davon betroffen*. Der Grund liegt meist bei fehlenden oder unzureichenden Sicherheitsvorkehrungen.

Denn oft reicht schon ein Klick, eine kurze Unaufmerksamkeit oder eine inaktive Firewall und schon ist es passiert. Die Folgen sind meist enorm – für viele KMUs sogar existenzbedrohend. Cyber-Attacken bringen aber nicht nur hohe finanzielle Schäden mit sich, sondern verursachen auch erhebliche Image- und Reputationsverluste.

Strengere gesetzliche Datenschutzregelungen

Seit Mai 2018 gilt die neue Datenschutzgrundverordnung (DSGVO). Diese sieht verschärfte Regeln beim Datenschutz vor. Werden beispielsweise Persönlichkeits- oder Datenschutzrechte verletzt, können hohe Schadenersatzverpflichtungen anfallen.

Digitaler Arbeits-Alltag wird immer komplexer

Aber nicht nur Internet-Gefahren oder gesetzliche Änderungen bereiten Unternehmen Kopfzerbrechen. Oft ist es auch die eigene IT-Ausstattung, die Probleme mit sich bringt. Egal, ob Drucker, PC, Server, Datenverarbeitungsprogramm oder Backup-System – die IT-Struktur wird immer komplexer. Viele KMUs sind jedoch zu klein, um Fachkräfte fix anzustellen.

Einfallstore**:

Der Cyber-Angriff erfolgte durch...



Schäden**:

Die Angriffe führten zu wirtschaftlichen Schäden durch¹...



* techbold, Studie „IT-Sicherheit KMU 2018 in Österreich, www.techbold.at:

** Gesamtverband der Deutschen Versicherungswirtschaft (GDV), Forsa-Befragung. Frühjahr 2018 „Cyberisiken im Mittelstand, www.gdv.de

¹ Mehrfachnennungen möglich

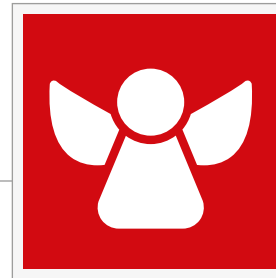
Keine Sorgen IT-Sicherheitspaket

Unsere Lösung – Ihr Schutz in der digitalen Welt

Unser innovatives Keine Sorgen IT-Sicherheitspaket ist eine individuelle Lösung für Ihr Klein- und Mittelunternehmen. Damit unterstützen wir Sie bei alltäglichen IT-Problemen und helfen Ihnen mögliche Schäden durch Cyber-Angriffe zu minimieren und deren finanziellen Folgen abzuwenden. Wir verbinden Service, Dienstleistung und Versicherung in unserem einzigartigen Keine Sorgen IT-Sicherheitspaket.

Woraus besteht unser Keine Sorgen IT-Sicherheitspaket?

- 1 IT-Basis Scan**
Wir prüfen Ihre IT-Sicherheit auf offensichtliche Schwachstellen, erkennen damit mögliche Angriffspunkte und helfen Ihnen diese zu schließen.
- 2 Keine Sorgen Schutzengel**
24/7-Support bei IT-Fragen oder im Cyber-Notfall. Die Spezialisten in der Notrufzentrale sind Ihre erste Anlaufstelle bei IT-Problemen oder nach einem Cyber-Angriff.
- 3 Cyber-Versicherung**
Diese bietet umfassenden Schutz vor den finanziellen Folgen einer Cyber-Attacke – individuell an Ihr Unternehmen angepasst.



Ihre Vorteile auf einen Blick:

- 24/7-Support bei IT-Fragen oder im Cyber-Notfall per Telefon oder Fernwartung (Remote-Verbindung)
- Analyse möglicher Angriffspunkte von außen auf Ihr IT-System inkl. Verbesserungsvorschlägen
- Entfernung von Schadprogrammen
- Datenwiederherstellung inkl. Kostenübernahme
- IT-Forensik nach Cyber-Attacken inkl. Kostenübernahme: Ursachenforschung, Analyse und Aufarbeitung
- Finanzieller Schutz nach Cyber-Attacken: Eigen- & Fremdschäden
- Optionale Zusatzbausteine: Kostenersatz bei Betriebsunterbrechung, Krisen- & PR-Management bei Imageschäden, Vertragsstrafen etc.
- Zusammenarbeit mit hochqualifizierten Spezialisten aus den Bereichen IT, Recht, Krisen- und PR-Management

IT-Basis Scan

Wie sicher ist Ihr IT-System?



Cyber-Risiken zu erkennen wird immer schwieriger. Nicht nur die Anzahl und die Art von Cyber-Angriffen steigt ständig, sondern auch die Professionalität der Angreifer. Doch viele Sicherheitslücken können vorab durch kleine Maßnahmen geschlossen werden.

Wir prüfen Ihre IT-Sicherheit auf offensichtliche Schwachstellen, erkennen damit mögliche Angriffspunkte und helfen Ihnen diese zu schließen. Zusätzlich durchforsten wir das World Wide Web und das Darknet auf Hinweise, ob Cyber-Angriffe auf Ihr Unternehmen geplant sind.

Was prüft der IT-Basis Scan?

Ihr E-Mail

- Wie sicher ist Ihr beruflicher E-Mail-Account?
- Gibt es Schutz gegen Phishing (Ausspähen von Daten und Passwörtern)?

Ihre Website

- Können Besucher Ihrer Website einfach „gekapt“ und z. B. auf andere Websites weitergeleitet werden?
- Können Seiten-Inhalte so verändert werden, dass sie zu Schäden bei Dritten führen könnten?

Darknet

- Gibt es bereits verdächtige Angriffsmuster auf Ihr Unternehmen?
- Gibt es Hinweise (z. B. E-Mail-/Passwortlisten), die auf einen bereits erfolgten Angriff hindeuten?

Attack-Surface – Angriffspunkte Ihrer IT-Ausstattung

- Gibt es z. B. offene Ports oder veraltete Zertifikate, die einen Angriff auf Ihren Computer, Ihr System oder Ihr Netzwerk ermöglichen?



Keine Sorgen Schutzengel

Support bei IT-Fragen oder im Cyber-Notfall



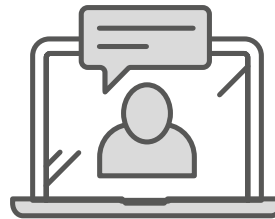
IT-Probleme oder Cyber-Angriffe halten sich nicht an Geschäftszeiten. Sie passieren auch nachts, an Wochenenden und Feiertagen. Wenn es plötzlich zu Ausfällen kommt, ist rasche Hilfe gefragt.

Keine Sorgen, die Mitarbeiter in der Notfallzentrale sind rund um die Uhr für Sie da. Sie kümmern sich sofort um Ihr IT-Problem und veranlassen alles Nötige – und das nicht nur bei oder nach einer Cyber-Attacke. Das spart Zeit, Geld und schont Ihre Nerven.



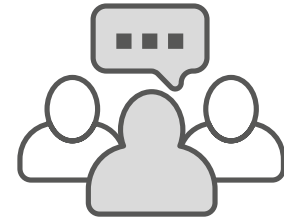
HILFE PER TELEFON

+43 800 20 39 390



HILFE PER FERNWARTUNG

Um das Problem zu lösen, verbindet sich der IT-Spezialist mit Ihrer Hardware (PC, Laptop, Smartphone) – natürlich nur mit Ihrem Einverständnis.



HILFE VOR ORT

In seltenen Fällen oder nach einem Cyber-Angriff kann es sein, dass ein Spezialist in Ihr Unternehmen kommen muss. Auf Wunsch wird dieser von der Notrufzentrale organisiert.

Die IT-Spezialisten helfen und beraten z. B. bei

- der Umsetzung der Verbesserungsmöglichkeiten aus dem IT-Basis Scan
- alltäglichen Problemen mit Ihrer KMU-typischen Hard- und Software (First-Level-Support)
- der Installation und Wartung von Hard- und Software
- Problemen mit Ihrem Internetzugang
- der Prüfung Ihrer Website z. B. auf Rechtskonformität oder Barrierefreiheit
- Cyber-Crime, z. B. Phishing, Identitätsdiebstahl oder Cyber-Mobbing
- der Organisation einer kostenlosen Rechtsberatung bei Cyber-Crime (max. 1 h pro Kalenderjahr)
- der Organisation aller nötigen Maßnahmen im Falle einer Cyber-Attacke

Cyber-Versicherung

Finanzieller Schutz nach Cyber-Angriffen und Datenschutzverletzungen



100%-igen Schutz gibt es nicht. Aber Keine Sorgen: Sollte es trotz aller Vorkehrungen zu einem Cyber-Angriff oder einer Datenschutzverletzung kommen, bietet die inkludierte Cyber-Versicherung finanziellen Schutz.

Diese deckt nicht nur Schäden in Ihrem Unternehmen, sondern auch Schäden bei Dritten, für die Ihr Unternehmen gesetzlich haftet. Die Cyber-Versicherung kann auf Wunsch erweitert und an Ihr Unternehmen angepasst werden.

Was ist versichert?

Versichert sind reine Vermögensschäden aufgrund

- eines Cyber-Angriffes,
- eines unberechtigten Zugriffs (z. B. eines Mitarbeiters) oder
- einer Datenschutzverletzung.

Mögliche Versicherungssummen:

- EUR 100.000,-
- EUR 250.000,-

Fixer Selbstbehalt (gilt nur für die Cyber-Versicherung):

- Wahlweise: EUR 1.000,-, EUR 2.000,- oder EUR 5.000,-

Im Basisschutz dabei:

- Forensik- und Schadenfeststellungskosten
- Datenwiederherstellungskosten inkl. Entfernung der Schadsoftware
- Call-Center-Kosten nach einer Datenschutzverletzung
- Benachrichtigungskosten nach einer Datenschutzverletzung
- Erfüllung berechtigter und Abwehr unberechtigter Schadenersatzforderungen Dritter
- Erfüllung von Schadenersatzverpflichtungen wegen einer Verletzung des Persönlichkeitsrechts, einer Namensrechtsverletzung oder Urheber- und Markenrechtsverletzung

Optionale Erweiterungen:

- Betriebsunterbrechung mit Selbstbehalt
- Kosten für die Einschaltung eines Krisenmanagements oder PR-Beraters zur Wiederherstellung der öffentlichen Reputation
- Vertragsstrafen wegen einer Verletzung des Payment Card Industry (PCI) Datensicherheitsstandards
- Vertragliche Schadenersatzansprüche



So hilft das Keine Sorgen IT-Sicherheitspaket

Beispiele aus der Praxis

IT-Problem im Friseursalon

IOS Kalender auf neuem Android-Device

Ein kleiner Friseursalon verwaltete seine Kundentermine über ein iPad. Nach dem Umstieg auf ein Android-Tablet wurden die vorhandenen Termine nicht mehr im Kalender angezeigt.

Auswirkungen

- ✘ Es kam zu Überschneidungen von Terminen und es entstanden sehr lange Wartezeiten für die Kunden.
- ✘ Kunden beschwerten sich über das Chaos bei der Terminvergabe und drohten, einen neuen Friseur zu suchen.

Leistungen des IT-Sicherheitspakets

- ✓ Der Mitarbeiter in der Notfallzentrale verbindet sich mittels Remote-Verbindung (Fernwartung) mit einem Laptop im Friseursalon.
- ✓ Der Spezialist installierte AnyTrans auf dem Laptop und erstellte ein neues Google-Konto. Beide Geräte (iPad und Android-Tablet) wurden mittels USB-Kabel am Laptop angeschlossen.
- ✓ Der Mitarbeiter richtete das Google-Konto auf dem neuen Tablet ein, synchronisierte und importierte alle Kalender-Einträge sowie die Kontakte.



Cyber-Angriff auf ein Autohaus

Hacking des Servers mittels E-Mail-Anhang

Ein Verkaufsmitarbeiter öffnete versehentlich einen E-Mail-Anhang, der einen Virus enthielt. Die Schadsoftware manipulierte den Firmenserver und versendete über die IT-Infrastruktur tausende Spam-E-Mails.

Auswirkungen

- ✘ Das Autohaus musste mit vielen Beschwerden von Kunden und Partnern umgehen.
- ✘ Die IT des Autohauses war mit einem Trojaner infiziert. Erst nach knapp einer Woche konnte der Versand von Spam-E-Mails gestoppt werden.

Leistungen des IT-Sicherheitspakets

- ✓ Ein Daten-Forensiker wurde beauftragt, um die Ursache für den Versand von Spam-E-Mails zu finden.
- ✓ Ein IT-Spezialist bereinigte das System vor Ort vom Trojaner.
- ✓ Die Kosten in Höhe von EUR 9.000,- für den IT-Forensiker und die Entfernung der Schadsoftware wurden von uns übernommen – lediglich der gewählte Selbstbehalt wurde in Abzug gebracht.

Weitere Beispiele finden Sie auf www.keinesorgen.at/it-paket



Haben Sie dazu noch Fragen?
Nähere Infos auf www.keinesorgen.at/it-paket

Ober  **österreichische**
www.keinesorgen.at