

A person wearing a dark hoodie is the central focus, set against a background of a city skyline and silhouettes of people walking. The image has a red and blue color scheme with a digital, glitch-like effect.

**Unser IT-
Sicherheitspaket.**

**Dein
optimaler
Schutz.**

ober 
österreichische
versicher.at

Cyber-Kriminalität, Datenschutz und IT-Probleme

Darum ist eine Absicherung wichtig

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 2018 bis 2022 stieg die Anzahl angezeigter Cyber-Crime-Fälle österreichweit von 19.627 auf 60.195 an.*

Es geht so schnell – KMUs besonders stark betroffen

Die Aussage, dass Klein- und Mittelunternehmen (KMUs) seltener angegriffen werden, ist schlichtweg falsch. Cyber-Kriminelle suchen primär nach verwundbaren Systemen, dringen ein und schauen erst dann, ob und was sie für sich herausholen können. Cybersicherheit ist teilweise zu einem Wettbewerb geworden. Oftmals wird versucht durch eine bessere Cyber-Sicherheit als andere Unternehmen nicht in den Fokus Cyber-Krimineller zu fallen. 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. Sie verursachen auch erhebliche Image- und Reputationsverluste.

Angriff mit Auswirkungen

Nahezu jedem zehnten attackierten österreichischen Unternehmen entstehen durch Cyber-Kriminelle finanzielle Schäden von mehr als EUR 1.000.000,-.**

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. Das Problem: Viele KMUs sind zu klein, um IT-Fachkräfte anzustellen.

Cyber-Angriffe nehmen jährlich zu**:

- 12 %** erlitten einen finanziellen Schaden von mehr als EUR 1.000.000,-
- 33 %** mussten eine Betriebsunterbrechung von rund einer Woche aufgrund eines Ransomware-Angriffs in Kauf nehmen
- 55 %** sehen durch Cyberangriffe ihre geschäftliche Existenz bedroht
- 25 %** wurden über private soziale Netzwerke versucht zu beeinflussen, die auf das berufliche Umfeld abzielten
- 33 %** waren Opfer von Ransomware/Erpressung
- 22 %** waren in den vergangenen zwölf Monaten von Deep-fakes betroffen

Die häufigsten Arten von Cyber-Angriffen**:

Identitätsdiebstahl	490 %
Advanced Persistent Threats (APTs)	240 %
Insider Threat	240 %
Datendiebstahl (Data Breach)	229 %
Social Engineering.	200 %
Malware (E-Mail-Anhang)	140 %
Ransomware/Erpressung	136 %
Denial of Service-Attacken (DoS).	124 %
Business E-Mail Compromise, CEO/CFO Fraud.	115 %
(Spear) Phishing-Attacke (E-Mail-Link).	92 %

* Cybercrime Report des Bundeskriminalamts, ** KPMG, Cyber Security in Österreich

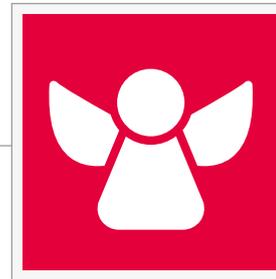
Keine Sorgen IT-Sicherheitspaket

Unsere Lösung – Ihr Schutz in der digitalen Welt

Unser IT-Sicherheitspaket ist eine spezielle Lösung für Ihr Klein- oder Mittelunternehmen. Dabei kombinieren wir Service, Dienstleistung und Versicherung in einem optimalen Versicherungsprodukt.

Woraus besteht unser IT-Sicherheitspaket?

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



Ihre Vorteile im Überblick:

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

Absicherung nach Cyber-Angriffen & Datenschutzverletzungen



100%-igen Schutz gibt es nicht. Sollte es trotzdem 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, sofern Sie dafür haften. 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,-
- EUR 500.000,-
- EUR 1.000.000,-

Fixer Selbstbehalt in der Cyber-Versicherung:

- Wahlweise: EUR 1.000,-, EUR 2.500,-, EUR 5.000,- oder EUR 10.000,-

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



24/7-Support bei Cyber-Angriffen oder IT-Problemen



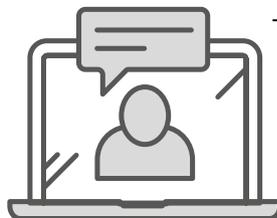
IT-Probleme oder Cyber-Angriffe halten sich nicht an Geschäftszeiten. Sie passieren auch nachts, an Wochenenden und Feiertagen. Wenn es plötzlich zu Ausfällen kommt, ist rasche Hilfe gefragt.

Die Mitarbeiter in der Notfallzentrale sind rund um die Uhr für Sie da. Ob Cyber-Angriff oder IT-Problem – der 24/7-Support hilft sofort und veranlasst alles Nötige. Das spart Zeit, Geld und schont Ihre Nerven.



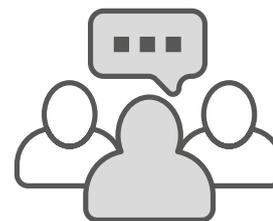
HILFE PER TELEFON

+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 von Verbesserungsmöglichkeiten aus den Ergebnissen des IT-Sicherheits-Checks
- 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 Stunde/Jahr)
- der Organisation aller nötigen Maßnahmen im Falle einer Cyber-Attacke

IT-Sicherheits-Check (Optional)

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. Was oft vergessen wird: Viele Sicherheitslücken können bereits im Vorfeld durch kleine Maßnahmen geschlossen werden.

Mit unserem IT-Sicherheits-Check prüfen wir punktuell Ihre IT-Sicherheit auf offensichtliche Schwachstellen, erkennen damit mögliche Angriffspunkte und helfen Ihnen diese zu schließen. Ausserdem scannen wir das World Wide Web und das Darknet auf Hinweise, ob Cyber-Angriffe auf Ihr Unternehmen geplant sind. Selbstverständlich wird bei jeglichen Prozessen die Anonymität Ihres Unternehmens gewahrt.



Was prüft der IT-Sicherheits-Check?

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 „gekapert“ und z. B. auf andere Websites weitergeleitet werden?
- Können Seiteninhalte so manipuliert werden, dass sie zu Schäden bei Dritten führen könnten?

Darknet

- Gibt es bereits verdächtige Angriffsmuster?
- 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?

So hilft das IT-Sicherheitspaket

Beispiele aus der Praxis*

Cyber-Angriff auf eine Kanzlei

Verschlüsselte Daten durch schwaches Passwort

Durch ein schwaches Passwort wurde das Computersystem einer Anwaltskanzlei mit einer Schadsoftware infiziert. Der Krypto-Trojaner verschlüsselte sämtliche Dateien – inkl. dem E-Mail-Archiv. Eine Mitarbeiterin informierte den eigenen IT-Berater. Dieser befand sich aber im Urlaub. Die Mitarbeiterin verständigte danach sofort unsere 24/7-Notfallzentrale.

Auswirkungen

- ✘ Die Kanzlei konnte nicht mehr auf ihre Dateien zugreifen. Die Weiterarbeit war stark eingeschränkt. Fast alles musste telefonisch erledigt werden.
- ✘ Auch das Backup wurde durch den Trojaner beschädigt. Eine aufwendige Daten-Rekonstruktion war notwendig.
- ✘ Es dauerte fast zwei Wochen, bis alles wieder einwandfrei funktionierte.

Leistungen des IT-Sicherheitspakets

- ✓ Die Notfallzentrale verständigte sofort IT-Sicherheitsexperten, die sich vor Ort um das Problem kümmerten und den Trojaner unschädlich machten.
- ✓ Sämtliche Daten konnten wiederhergestellt werden. Die Kosten in Höhe von knapp EUR 36.000,- wurden von uns übernommen. Die Kanzlei musste nur für den gewählten Selbstbehalt aufkommen.



* Die angeführten Schadenbeispiele dienen der Veranschaulichung unseres Versicherungsproduktes und sind zur besseren Verständlichkeit unserer Versicherungsleistungen gekürzt und vereinfacht dargestellt. Deckungsansprüche aufgrund der Schadenbeispiele können nicht geltend gemacht werden.



IT-Problem in der Kfz-Werkstatt

Drucker nach Update funktionslos

Ein automatisches Update legte den einzigen und zuvor funktionierenden Drucker einer Kfz-Werkstatt lahm. Scannen, Drucken und Kopieren war über alle Computer nicht mehr möglich. Kostenvoranschläge, Reparaturberichte und Rechnungen konnten nur sehr eingeschränkt weiterverarbeitet werden. Die Werkstatt meldete den Vorfall sofort unserer 24/7-Notfallzentrale.

Auswirkungen

- ✘ Das Tagesgeschäft war teilweise unterbrochen bzw. stark beeinträchtigt, da viele Aufträge nicht abgeschlossen werden konnten.
- ✘ Es kam zu langen Wartezeiten – ganz zum Ärger der Kunden. Diese drohten die Werkstatt zu wechseln.

Leistungen des IT-Sicherheitspakets

- ✓ Der Mitarbeiter in der Notfallzentrale verband sich mittels Remote-Verbindung (Fernwartung) mit einem PC in der Kfz-Werkstatt.
- ✓ Er prüfte sämtliche Einstellungen am Computer und am Drucker.
- ✓ Danach installierte er die aktuellsten Treiber und konfigurierte den Drucker neu – Problem gelöst. Anschließend wurden noch alle anderen Computer neu eingerichtet.

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



Haben Sie Fragen?

Ihre Beraterin oder Ihr Berater ist gerne für Sie da.

Nähere Infos auch auf www.versich.at/it-paket

oder unter +43 5 78 91-0.

Diese Marketingmitteilung enthält kurze, überblicksartige Informationen zum Produkt. Sie ist kein Angebot im rechtlichen Sinn. Vollständige und verbindliche Informationen finden Sie in den Antragsunterlagen und Versicherungsbedingungen. Medieninhaber: Oberösterreichische Versicherung AG, Linz. Hersteller: [Salzkammergut Druck Mittermüller, Gmunden](#). Druckfehler und Irrtum vorbehalten. [039334](#) - Stand 04/24.

ober 
österreichische
versich.at