

Homeoffice:
Gefahren
für Ihre
IT-Sicherheit



IT-Sicherheit im Griff?

Gesetzliche Pflichten, verständliche
Analysen & Tipps fürs Homeoffice



IT-Sicherheit ist Chefsache

Stellen Sie sich vor, Sie kommen morgens in Ihr Büro, schalten den Computer ein – und sehen nur einen schwarzen Bildschirm mit einer Lösegeldforderung. Keine Kundendaten, keine Rechnungen, keine Produktion. Alles steht still.

Für viele kleine und mittlere Unternehmen (KMU) ist das kein theoretisches Szenario mehr, sondern bitterer Alltag. Das Risiko, Opfer einer Cyberattacke zu werden, war noch nie so hoch wie heute. Dabei gilt: Unwissenheit schützt vor Strafe und Schaden nicht, denn als Geschäftsführer oder Inhaber stehen Sie in der Verantwortung. IT-Sicherheit ist keine lästige Aufgabe, sondern eine existenzielle Pflicht für die Unternehmensführung.

Dennoch sind viele Inhaber und Geschäftsführer von kleinen und mittleren Unternehmen überzeugt, dass ihr Unternehmen für Hacker uninteressant sei. Ein gefährlicher und existenzbedrohender Irrtum. Mehr als 80 % aller Cyberangriffe im Mittelstand betreffen Unternehmen, die nichts mit IT zu tun haben, aber im Alltag komplett von ihr abhängig sind – vom Handwerksbetrieb über den Online-Händler bis zur Arztpraxis.

Die bittere Realität: warum KMU im Visier stehen
Cyberkriminelle greifen heute selten gezielt einzelne Firmen an. Sie nutzen automatisierte Software-Bots, die

das Internet flächendeckend nach Sicherheitslücken durchsuchen. Finden sie ein offenes Tor, schlagen sie zu. Die häufigsten Einfallstore in KMU sind:

- ✓ **Veraltete Software:** Fehlende Sicherheitsupdates bei Betriebssystemen oder Programmen sind wie eine offenstehende Haustür.
- ✓ **Der Faktor Mensch:** Phishing-E-Mails werden immer professioneller. Ein falscher Klick eines Mitarbeiters genügt, um das gesamte Netzwerk zu infizieren.
- ✓ **Fehlende Netztrennung:** Wenn das private Smartphone im selben WLAN funkt wie der Server mit den sensiblen Kundendaten, ist das Risiko vorprogrammiert.

Gesetzliche Pflichten für Unternehmen

Als Unternehmer haften Sie für die Sicherheit in Ihrem Betrieb. Die Gesetzgebung (unter anderem durch die DSGVO und verschärfte EU-Richtlinien) nimmt die Führungsebene unmissverständlich in die Pflicht.

1. Die Pflicht zur Risikovorsorge:

Geschäftsführer müssen existenzbedrohende Risiken – und dazu gehören Cyberangriffe – rechtzeitig erkennen und minimieren. Wer das Thema ignoriert, handelt im Schadensfall organisatorisch fahrlässig.

2. Persönliche Haftung:

Bei schweren Versäumnissen in der IT-Sicherheit droht im Ernstfall die persönliche Haftung des Geschäftsführers mit dem Privatvermögen.

3. Verlust des Versicherungsschutzes:

Cyber-Versicherungen zahlen im Schadensfall nur dann, wenn das Unternehmen nachweisbare Mindeststandards bei der IT-Sicherheit eingehalten hat.

4. Schutz von Kundendaten:

Die DSGVO fordert den lückenlosen Nachweis „geeigneter technischer und organisatorischer Maßnahmen“ (TOM). Bei Datenpannen drohen horrende Bußgelder.

Betriebs-IT gegen Angriffe von außen sichern

Der Schutz Ihres Unternehmens erfordert kein Informatik-Studium, sondern ein systematisches Vorgehen. Diese fünf Kernbereiche muss jedes KMU im Griff haben:

1. Starke Passwörter & Zwei-Faktor-Authentisierung

(2FA): Passwörter allein reichen nicht mehr aus. Ein zweiter Bestätigungscode auf dem Smartphone (2FA) blockiert fast 99 % aller automatisierten Konto-Übernahmen.

2. Professionelles Backup-Konzept:

Ihre Daten müssen täglich und automatisiert gesichert werden. Wichtig: Die Sicherung muss physisch oder logisch vom restlichen Netzwerk getrennt sein, damit Hacker die Backups nicht mitverschlüsseln können.

3. Firewall & Netzwerk-Struktur:

Eine professionelle Firewall überwacht den Datenverkehr von außen. Sensible Bereiche (wie die Buchhaltung) sollten vom restlichen Netzwerk isoliert sein.

4. Regelmäßige Updates:

Sicherheitspatches müssen sofort eingespielt werden – auf Servern, PCs und allen Mobilgeräten.

5. Mitarbeiter-Sensibilisierung:

Schulen Sie Ihr Team. Wer weiß, wie eine gefälschte Rechnung oder eine Phishing-Mail aussieht, drückt im Ernstfall nicht auf „Öffnen“.

Der Weg zur Sicherheit: das Ende der Zettelwirtschaft

Eigentlich klingt es einfach: Man lässt den Ist-Zustand der IT-Infrastruktur aufnehmen, prüft die Risiken und leitet klare Empfehlungen ab. In der Realität scheitert es jedoch oft daran, dass jeder Techniker anders arbeitet. Fragen, Schwerpunkte und Dokumentationen variieren. Am Ende entsteht eine unübersichtliche Zettelwirtschaft. Risiken werden uneinheitlich bewertet, Ergebnisse sind kaum vergleichbar und Angebote für Sicherheitslösungen bleiben schwammig.

Das geht auch anders. Um Ihnen als Unternehmer absolute Gewissheit und glasklare Transparenz zu bieten, arbeiten wir nach einer standardisierten, zertifizierten Methode der SYNAXON Managed ISA Plus.

Dabei wird Ihre IT-Landschaft strukturiert und digital analysiert – ganz ohne IT-Kauderwelsch. Das Besondere: Diese Analyse basiert auf mehr als 200 praxisrelevanten Fragen sowie den 27 strengen Anforderungen nach DIN SPEC 27076 für den Cyber-Risiko-Check (nach Standards des BSI IT-Grundschutzes).

Das Ergebnis für Ihr Unternehmen

Glasklarer Analysebericht: Sie erhalten eine verständliche Management-Übersicht, die die Schwachstellen Ihrer IT sofort sichtbar macht.

Rechtliche Absicherung: Sie dokumentieren schwarz auf weiß, dass Sie Ihren Pflichten als Unternehmer nachkommen.

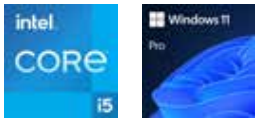
Gezielte Investition: Sie investieren nur in die Sicherheitslösungen, die Sie wirklich brauchen.

Sie haben Interesse an einer standardisierten Infrastrukturanalyse? Dann nehmen Sie Kontakt zu uns auf.

Sprechen Sie uns an!

Lenovo

Zuverlässige Partner für die alltäglichen Aufgaben



**15,6" FULL HD-DISPLAY
(39,6 CM, IPS, BLENDFREI)**

MILITÄRSTANDARD-GEPRÜFT (MIL-STD-810H)

SCHNELLES WI-FI 6 & 16 GB DDR5 RAM

NUMMERNBLOCK & PRIVACY-WEBCAM

LENOVO V15 G5 IRL

Intel® Core™ i5-13420H Prozessor (bis zu 4,60 GHz mit Intel® Turbo-Boost-Technik, 12 MB Intel® Cache) | 16 GB RAM 512 GB SSD | Intel® UHD Graphics | Schnittstellen u. a. USB, USB-C (unterstützt DisplayPort Alt Mode), HDMI, LAN, Audio integrierte Webcam-Abdeckung | Windows 11 Pro

Preis auf Anfrage



Preise und Verfügbarkeiten auf Anfrage. Aufgrund der aktuellen Marktsituation beraten wir Sie gern persönlich zu Ihrem Wunschprodukt.

AMD



**16" WUXGA-DISPLAY
(40,6 CM, IPS, BLENDFREI)**

TASTATUR MIT HINTERGRUNDBELEUCHTUNG

FINGERPRINT & FHD-IR-KAMERA (WINDOWS HELLO)

LOW-BLUE-LIGHT-TECHNOLOGIE

LENOVO ThinkBook 16 G7 ARP

AMD Ryzen™ 7 7735HS Prozessor (bis zu 4,75 GHz, 16 MB Cache) | 32 GB RAM | 1 TB SSD | AMD Radeon™ 680M Grafikeinheit | Schnittstellen u. a. USB, USB-C (unterstützt DisplayPort Alt Mode), USB4 (unterstützt DisplayPort Alt Mode), HDMI, LAN, Audio | Fingerprint-Reader, integrierte Webcam-Abdeckung | Windows 11 Pro

Preis auf Anfrage



Bestens ausgestattet für Ihr Business

**HÖHENVERSTELL- UND NEIGBAR
MIT PIVOT-FUNKTION**

**INTEGRIERTER USB-HUB UND
LAUTSPRECHER**

LOW-BLUE-LIGHT-TECHNOLOGIE

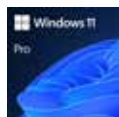
LENOVO ThinkVision T24d-30

Auflösung: 1.920 x 1.200 Pixel im
Format 16:10 bei 100 Hz Kontrast: 1.500:1
(dynamisch 3 Mio:1) | Helligkeit 300 cd/m²
Reaktionszeit 4 ms (Extreme Mode)
VGA, HDMI, DisplayPort, USB, Audio

Preis auf Anfrage



**Nicht das Passende gefunden? Fragen Sie uns nach einem Angebot
für Ihre individuellen unternehmerischen Anforderungen!**



INTEGRIERTE LAUTSPRECHER

**INKLUSIVE USB-TASTATUR &
MAUS**

**MILITÄRSTANDARD-GEPRÜFT
(MIL-STD-810H)**

LENOVO ThinkCentre M75t G5

AMD Ryzen™ 5 8500G Prozessor
(bis zu 5,00 GHz, 16 MB Cache)
16 GB RAM | 512 GB SSD | AMD
Radeon™ 740M Grafikeinheit
Schnittstellen u. a. USB, USB-C,
DisplayPort, HDMI, LAN, Audio
Abmessungen: 145 x 296 x 346 mm
(BxTxH) | Windows 11 Pro

Preis auf Anfrage



**PASSENDE DOCKINGSTATION
GLEICH DAZU KAUFEN**



LENOVO ThinkPad Universal USB-C Dock

Schnittstellen u. a. USB, USB-C, DisplayPort, HDMI, LAN, Audio
Gewicht: 340 Gramm | 90 Watt

Preis auf Anfrage

Hybrides Arbeiten im Visier

So machen Sie das Homeoffice sicher

Das Arbeiten von zu Hause aus ist aus unserem Arbeitsalltag nicht mehr wegzudenken. Es bietet Flexibilität für Mitarbeiter und handfeste Vorteile für Unternehmen. Doch was für die Work-Life-Balance ein Segen ist, hat sich für Cyberkriminelle zum absoluten Hauptgewinn entwickelt. Das Homeoffice ist heute eines der größten Einfallstore für Angriffe auf die gesamte Betriebs-IT.

Das Risiko steigt: Cybercrime im modernen Gewerbe

Aktuelle Lagebilder des Bundeskriminalamts (BKA) und des BSI zeigen eine klare Tendenz: Die Professionalität und Aggressivität von Cyberkriminellen nehmen von Jahr zu Jahr zu. Besonders gefährlich sind hochentwickelte Ransomware-Angriffe (Erpressertrojaner). Wird ein Firmennetzwerk erst einmal infiziert, drohen wochenlange Produktions- und Arbeitsausfälle. Oft bleibt den betroffenen Unternehmen am Ende nichts anderes übrig, als das gesamte Netzwerk unter enormem Kosten- und Zeitaufwand komplett neu aufzubauen.

Der Brandbeschleuniger im privaten Netzwerk

Warum ist das Arbeiten im Homeoffice so gefährlich? Im Büro schützt eine zentrale, professionelle Firewall die Systeme. Zu Hause fehlt dieser Schutzwall meist völlig. Zudem nutzen Angreifer psychologische Faktoren geschickt aus: Im Homeoffice fehlt der kurze Zuruf „Hast du mir diese Mail geschickt?“ über den Flur zur Kollegin. Phishing-Angriffe per E-Mail, Messenger oder über gefälschte Rechnungen sind heute so täuschend echt, dass ein unachtsamer Klick genügt, um Schadsoftware unbemerkt ins Firmennetzwerk einzuschleusen.

Eine der häufigsten technischen Schwachstellen ist das sogenannte Remote-Desktop-Protokoll (RDP) sowie Fernwartungssoftware. Diese Tools ermöglichen es Mitarbeitern, von außen auf ihren Büro-PC oder den Firmenserver zuzugreifen.

Das Problem: Sind diese Zugänge schlecht abgesichert, unverschlüsselt oder ohne zusätzlichen Schutz über das offene Internet erreichbar, ist das für Hacker eine Einladung

mit rotem Teppich. Ein erfolgreicher Knackpunkt am RDP-Zugang öffnet Angreifern sofort das Tor zum Herzstück Ihres gesamten Unternehmens.

Arbeitsrecht & IT-Sicherheit: feste Regeln für Ihr Team

Sicherheit im Homeoffice ist kein reines IT-Thema, sondern erfordert klare Absprachen und Richtlinien. Experten sind sich einig: Ein Großteil der digitalen Angriffe lässt sich durch klare Verhaltensregeln und ein geschultes Team verhindern. Folgende Spielregeln sollten Sie in Ihrem Betrieb verbindlich festlegen:

- **Sensibilisierung statt Blindflug:**

Schulen Sie Ihr Team regelmäßig. Wer weiß, wie moderne Betrugsmaschinen aussehen, schützt das Unternehmen aktiv vor Schäden.

- **Das private WLAN absichern:**

Verpflichten Sie Mitarbeiter im Homeoffice, das Standard-Passwort ihres privaten WLAN-Routers zu





ändern und regelmäßige Geräte-Updates durchzuführen. Es sollte ein moderner Verschlüsselungsstandard (wie WPA3) aktiv sein.

- **Strikte Trennung von Privat und Beruf:**

Private USB-Sticks, externe Festplatten oder die private Cloud dürfen auf keinen Fall mit dem Firmen-Laptop genutzt werden. Umgekehrt gehört die geschäftliche Hardware niemals in die Hände von Familienmitgliedern.

- **Blicke Dritter verhindern:**

Der Küchentisch ist kein abgetrennter Büroraum. Mitarbeiter müssen dafür sorgen, dass weder Familienmitglieder noch Besucher Einblick in sensible Kundendaten oder Bildschirme erhalten.

- **Betriebsübliche Arbeitszeiten nutzen:**

Auch im Homeoffice gelten die normalen Arbeitszeiten. Das erleichtert nicht nur die Absprache im Team, sondern sorgt auch dafür, dass IT-Auffälligkeiten während der regulären Geschäftszeiten schneller vom Support bemerkt werden.

Halten Sie diese Regeln schriftlich in einer Homeoffice-Vereinbarung fest – denn IT-Sicherheit beginnt im Kopf jedes einzelnen Mitarbeiters.

Homeoffice sicher gestalten – sprechen Sie uns an!

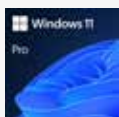
Vorsicht ist nachweislich besser und günstiger als Nachsicht. Wir unterstützen Sie dabei, die Arbeitsplätze Ihres Teams im Homeoffice technisch und organisatorisch absolut wasserdicht zu machen. Und sollten Sie bereits den Verdacht eines Cyberangriffs haben, sind wir sofort für Sie da.

**Interesse geweckt?
Kontaktieren Sie uns!**

GOGREEN

Wir versenden klimafreundlich
mit der Deutschen Post

Vielseitig wie Ihr Arbeitstag



LEISTUNGSSTARKE INTEGRIERTE KI

**BRILLANTES 120 HZ
PIXESENSE TOUCH-DISPLAY**

BIS ZU 14 STUNDEN AKKULAUFZEIT & WI-FI 7



**13" TOUCH-DISPLAY (33,0 CM, 2880 X
1920, 120 HZ, ENTSPIEGELT)**

 **Microsoft Surface**

MICROSOFT Surface Pro 11

Intel® Core™ Ultra 5 236V Prozessor (bis zu 4,70 GHz mit Intel® Turbo-Boost-Technik, 8 MB Intel® Cache) | 16 GB RAM | 512 GB SSD | Intel® Arc™ Grafik | Schnittstellen u. a. USB4 (unterstützt Thunderbolt), SurfaceConnect | Frontkamera: 1440p, Rückkamera: 10 Megapixel | Corning Gorilla Glass 5 Windows 11 Pro

Preis auf Anfrage



Copilot+PC



Stand 08/2026. Gültig bis 31. Oktober 2026. Solange der Vorrat reicht. Irrtümer und Preisänderungen vorbehalten. Alle Preise sind Euro-Preise zzgl. gesetzl. USt.
Bildnachweise: Die Bilder zu den redaktionellen Beiträgen sind KI-generiert – ChatGPT / OpenAI, 2026. Zur besseren Lesbarkeit verwenden wir in allen Texten die männliche Form; gemeint sind jedoch immer alle Geschlechter und Geschlechtsidentitäten.



avanito

advanced it solutions

avanito GmbH | Im Weiherfeld 8 | 85051 Ingolstadt
Telefon +49 8450 32997-0 | Fax +49 8450 32997-99 | E-Mail info@avanito.de
Internet www.avanito.de