

TECHNIK. BUSINESS. TRENDS.

IT insider

Digitaler Wandel – Wie KMU Schritt halten

Grüne IT für KMU

Nachhaltigkeit durch
Digitalisierung

Cloud Computing

Basis für flexible und
skalierbare Lösungen

Die Rolle der Mitarbeiter

Digitale Skills für den Wandel



Sehr geehrte Damen und Herren, liebe Geschäftspartner,

der digitale Wandel ist längst kein Zukunftsthema mehr – er findet jetzt statt. Für kleine und mittlere Unternehmen bedeutet das vor allem eines: Schritt zu halten, ohne sich zu überfordern. Zwischen steigenden Anforderungen, knappen Ressourcen und neuen Technologien gilt es, den richtigen Weg zu finden.

Dieses Magazin zeigt, wie das gelingen kann. Es geht nicht um große Visionen, sondern um konkrete Ansätze: Prozesse effizienter gestalten, Arbeitsplätze modernisieren, IT-Sicherheit stärken und die Cloud sinnvoll nutzen. Gleichzeitig wird deutlich: Digitalisierung ist mehr als Technik. Sie betrifft auch Menschen, Zusammenarbeit und Unternehmenskultur.

Die gute Nachricht: Die Umsetzung muss nicht in einem einzigen Schritt erfolgen. Niemand muss alles auf einmal umsetzen. Wer gezielt dort ansetzt, wo der größte Nutzen entsteht, schafft Schritt für Schritt die Basis für nachhaltigen Erfolg. Diese Ausgabe unseres Kundenmagazins liefert Ihnen Impulse, Orientierung und praxisnahe Einblicke, wie KMU den digitalen Wandel aktiv gestalten können.

Nutzen Sie die Chance, digitalen Wandel für Ihr Unternehmen aktiv zu gestalten – und machen Sie ihn zu einem echten Wettbewerbsvorteil. Dabei unterstützen wir Sie gern.

Wir wünschen Ihnen eine aufschlussreiche Lektüre.

Stefan Schempp
Schempp GmbH

Impressum

Herausgeber

SYNAXON AG
Falkenstraße 31 | 33758 Schloß Holte-Stukenbrock
Telefon 05207 9299–200 | Fax 05207 9299–296
info@synaxon.com | www.synaxon.com

Redaktion

André Vogtschmidt (V.i.S.d.P.), Theresa Twillemeier

Ansprechpartner

André Vogtschmidt | andre.vogtschmidt@synaxon.de

Gestaltung

Janina Redlich

Druck

FLYERALARMS GmbH | Alfred-Nobel-Str. 18 | 97080 Würzburg
0931 46584–0 | 0931 46584–1080 | info@flyeralarm.de

Zur besseren Lesbarkeit verwenden wir in unseren Texten das generische Maskulinum, sprich die männliche Form. Gemeint sind jedoch immer alle Geschlechter und Geschlechtsidentitäten.

Bildnachweis: KI-generiert mit Midjourney sowie Motive von Adobe Stock.

Stand 06/2026. Irrtümer und Druckfehler vorbehalten.

Inhalt

Seite 4

Die digitale Transformation – Wo KMU stehen



Seite 8

Managed Services

Vorteile der Zusammenarbeit mit Dienstleistern

Seite 6

Automatisierung von Geschäftsprozessen

Effizienzsteigerung durch IT



Seite 10

Cloud Computing

Basis für flexible und skalierbare Lösungen



Seite 14

Modern Workplace

Digitale Arbeitsumgebungen im Fokus



Seite 18

Die Rolle der Mitarbeiter

Digitale Skills für den Wandel



Seite 21

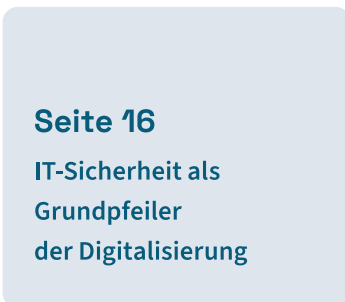
Grüne IT für KMU

Nachhaltigkeit durch Digitalisierung



Seite 16

IT-Sicherheit als Grundpfeiler der Digitalisierung



Die digitale Transformation

Digitale Transformation klingt oft nach Großkonzern, meint aber im Kern etwas ganz Bodenständiges: Technologie so einzusetzen, dass sie Ihnen im Arbeitsalltag den Rücken freihält. Ob Handwerksbetrieb oder Kanzlei – wer digitale Chancen nutzt, spart wertvolle Zeit und bleibt wettbewerbsfähig.

Zwischen Anspruch und Realität

Während große Unternehmen diesen Wandel oft strategisch und mit umfangreichen Ressourcen vorantreiben, zeigt sich im Mittelstand ein differenziertes Bild. Viele KMU sehen sich zwar »relativ gut aufgestellt«, doch echte digitale Vorreiter sind selten. Vor allem kleinere Betriebe haben Nachholbedarf – teilweise fühlen sie sich sogar abgehängt. Ein Grund: Ihnen fehlen häufig Zeit, Fachkräfte und Budgets, um die Digitalisierung konsequent umzusetzen.

Hürden im digitalen Alltag

Zu den größten Hürden zählen neben begrenzten Ressourcen auch bürokratische Anforderungen sowie Themen wie Datenschutz und IT-Sicherheit. Gerade Letzteres gewinnt an Bedeutung, da Cyberangriffe zunehmend als reale Bedrohung wahrgenommen werden. Gleichzeitig steigen die Erwartungen der Kunden: Sie wollen jederzeit, über jeden Kanal und möglichst einfach mit Unternehmen interagieren.

Pragmatismus schlägt Perfektionismus

Trotz dieser Herausforderungen bietet die digitale Transformation enorme Chancen. Viele KMU starten daher pragmatisch – etwa mit der Optimierung einzelner Prozesse. Automatisierung kann Routineaufgaben reduzieren, cloudbasierte Lösungen ermöglichen flexibles Arbeiten und digitale Tools verbessern die Zusammenarbeit sowie die Kundenansprache.

Mehr als nur ein IT-Projekt

Wichtig ist jedoch: Digitalisierung ist kein reines IT-Projekt. Der Erfolg hängt maßgeblich davon ab, ob Mitarbeiter eingebunden werden und ein kultureller Wandel stattfindet. Schulungen, klare Kommunikation und ein offener Umgang mit Veränderungen sind entscheidend, um Akzeptanz zu schaffen und Potenziale auszuschöpfen.

Für KMU gilt daher: Nicht den gesamten Betrieb über Nacht umkrempeln, sondern gezielt dort ansetzen, wo der größte Nutzen entsteht. Schritt für Schritt entsteht so ein digitales Fundament, das Effizienz steigert und die Wettbewerbsfähigkeit langfristig sichert. Lassen Sie uns gemeinsam dieses digitale Fundament errichten!



Kurz gesagt!

> Digitalisierung

Umwandlung analoger Informationen und Prozesse in digitale Formate, z. B. durch Software, Datenverarbeitung oder automatisierte Abläufe.

> Digitaler Wandel

Gesamtgesellschaftliche und wirtschaftliche Veränderungen durch digitale Technologien, die beeinflussen, wie Menschen arbeiten, kommunizieren und wirtschaften.

> Digitale Transformation

Umfassender strategischer Wandel eines Unternehmens, bei dem digitale Technologien alle Bereiche – von Prozessen über Geschäftsmodelle bis zur Unternehmenskultur – grundlegend verändern.

> Zusammengefasst

Ohne Digitalisierung keine digitale Transformation – und viele Transformationen treiben gemeinsam den digitalen Wandel voran.





Effizienzsteigerung durch IT

Automatisierung von Geschäftsprozessen

Was hält viele Führungskräfte nachts wach? Meistens sind es Wettbewerbsdruck und das Tempo, mit dem sich Kundenwünsche und Märkte wandeln. Wer mithalten will, braucht Abläufe, die nicht nur funktionieren, sondern sich flexibel anpassen lassen. Genau hier liegt der Hebel: Prozessautomatisierung macht Routinen planbar, reduziert Fehler und verschafft Ihnen Freiraum für echte Entscheidungen.

Schluss mit dem Flickenteppich

Geschäftsprozessautomatisierung (*Business Process Automation, BPA*) ist eine Strategie, bei der wiederkehrende und komplexere Abläufe mit Software automatisiert werden. Ziel ist ein reibungsloser Betrieb durch optimierte Tagesprozesse. Im Unterschied zu punktuellen Automatisierungen – also isolierten Einzellösungen für nur eine Aufgabe – verbindet BPA mehrere IT-Systeme und bildet durchgängige Ende-zu-Ende-Prozesse ab. Je nach Bedarf kommen Technologien wie Robotic Process Automation (*RPA*), Workflow-Orchestrierung, Business Process Management (*BPM*), Künstliche Intelligenz (*KI*) und Cloud-Plattformen zum Einsatz. So lassen sich Datenübergaben, Freigaben, Protokollierung und Eskalationen in einem durchgängigen Ablauf bündeln.

Entscheidend ist die Eignung des Prozesses: BPA spielt ihre Stärke dort aus, wo Abläufe repetitiv sind und klaren Regeln folgen. Ob ein Prozess reif für die Automatisierung ist, lässt sich am besten an seinen Auslösern, Entscheidungspunkten und Schnittstellen festmachen.

Geeignete Prozesse identifizieren

Automatisierung ist kein Allheilmittel für jede Ad-hoc-Aufgabe. Wenn redundante Schritte eliminiert und Abläufe sauber dokumentiert sind, stellt die Technik sicher, dass alles in der richtigen Reihenfolge und im vorgegebenen Zeitrahmen passiert.

Typische Merkmale passender Anwendungsfälle:

- > **Wiederkehrende Auslöser:** Ein Antrag, eine Bestellung oder ein Ticket stößt den Prozess an.
- > **Klare Wegweiser:** Es gibt definierte Punkte für Prüfungen, Freigaben oder Eskalationen.
- > **Saubere Daten:** Datenquellen und Schnittstellen sind eindeutig definiert.
- > **Messbarer Erfolg:** Durchlaufzeiten und Fehlerquoten lassen sich belegen.

Beispiele mit Soforteffekt

Viele Unternehmen starten dort, wo Zeitverluste direkt messbar sind und Übergaben häufig stattfinden.

Personalbeschaffung: Automatisierte Workflows beschleunigen die Vorprüfung und Terminabstimmung. Regelbasierte Zusagen oder Absagen sorgen für eine schnellere und konsistente Bewerberansprache.

Onboarding und Schulung: Standardabläufe steuern Unterlagen, Zugriffsrechte und Trainings rollenbasiert. Das minimiert Rückfragen und verkürzt die Einarbeitungszeit bis zur vollständigen Produktivität.



Zahlungs- und Abrechnungsprozesse:

Wiederkehrende Abrechnungen für Mitarbeiter und Externe laufen stabiler. Automatisierte Prüfungen reduzieren Fehler, während Freigaben lückenlos dokumentiert werden.

Personalplanung:

Abwesenheiten und Reisen werden abteilungsübergreifend synchronisiert. Engpässe sind früher sichtbar, Vertretungen besser planbar, HR wird von manueller Koordination entlastet.

Fakturierung:

Automatisierte Rechnungserstellung vermeidet Fehler und Inkonsistenzen. Zahlungsziele und Mahnstufen lassen sich präziser steuern. Das senkt rechtliche und finanzielle Risiken.

Kundenerfahrung:

Standardisierte Abläufe bei Anfragen und Eskalationen verkürzen Reaktionszeiten. Die konsistente Prozessführung reduziert Abbrüche und Wechselabsichten bei Verzögerungen.

Compliance und Regulierung:

Automatisierte Protokolle und Prüfpfade sichern eine nachvollziehbare Datenspur. Anforderungen für Audits lassen sich so in Echtzeit überwachen und einfacher belegen.

Was sich messbar verändert

Effizienz ohne Umwege:

Manuelle Arbeit, etwa über Tabellen, E-Mail-Schleifen und Medienbrüche, wird reduziert. Standardisierte Prozesse sind leichter zu verstehen, zu steuern und bei Wachstum zu skalieren. Gleichzeitig sinkt die Abhängigkeit von Einzelwissen.

Mehr Output, weniger Kosten:

Automatisierte Abläufe laufen konsistent mit geringerer Fehlerquote. Cloud-basierte BPA-Lösungen unterstützen zentrale Datenhaltung, ortsunabhängigen Zugriff und Echtzeit-Tracking. Das schafft Transparenz, verbessert Verantwortlichkeit und beschleunigt Entscheidungen.

Service auf neuem Level:

Reaktionszeiten sinken, Service wird zuverlässiger. Nachweise und Reports lassen sich bei Bedarf erzeugen und zeigen, welche Prozessschritte stabil funktionieren und wo Korrekturen nötig sind. Damit werden Verbesserungen messbar statt nur gefühlt.

Automatisierung ohne Stolpersteine

BPA scheitert selten allein an der Technik. Häufige Bremsen sind unklare Prozessverantwortung, fehlende Doku-

mentation oder zu viele Ausnahmen, die nie sauber definiert wurden. Auch die Skalierung ist anspruchsvoll: Was in einem Bereich funktioniert, lässt sich nicht automatisch auf andere Bereiche übertragen. Zudem muss das Zusammenspiel zwischen Menschen und Systemen klar geregelt sein, sonst entstehen Umgehungslösungen oder Schattenprozesse.

Wichtige Gegenmaßnahmen:

- > Prozesse vorab modellieren und Verantwortlichkeiten festlegen
- > Ausnahmen bewusst definieren statt »irgendwie lösen«
- > Schnittstellen und Datenqualität prüfen, bevor automatisiert wird
- > Schulungen und klare Betriebsregeln einplanen

Der Weg zur Prozessautomatisierung bietet große Chancen, erfordert aber einen sauberen Start und klare Prioritäten. Wenn Sie BPA einführen oder ausbauen möchten, sprechen Sie uns an. Wir identifizieren und priorisieren geeignete Prozesse und setzen diese technisch wie organisatorisch sauber um.



Managed Services

Stellen Sie sich vor, Sie kommen morgens in Ihren Betrieb, in Ihre Kanzlei oder in Ihre Praxis – und Ihre IT funktioniert einfach. Keine Fehlermeldungen, keine langsamen Rechner und vor allem kein ungutes Gefühl beim Thema Datensicherheit. Was für viele nach einem Idealzustand klingt, ist mit Managed Services längst Realität.

Digitalisierung braucht ein stabiles Fundament

Digitalisierung bedeutet heute weit mehr, als nur E-Mails zu schreiben. Es geht um digitale Patientenakten, vernetzte Baustellen oder rechtssichere Archivierung in der Cloud. Diese Möglichkeiten schaffen Effizienz und neue Spielräume, bringen aber auch wachsende Anforderungen an die IT mit sich.

Genau hier setzen Managed Services an: Sie sorgen dafür, dass Ihre technische Infrastruktur zuverlässig funktioniert, sicher bleibt und mit Ihren Anforderungen mitwächst.

Planbare Kosten statt unangenehmer Überraschungen

Klassischer IT-Service funktioniert häufig nach dem Prinzip: Ein Problem tritt auf, Sie rufen Hilfe, der Techniker kommt – und anschließend folgt eine Rechnung, deren Höhe sich vorher kaum abschätzen lässt. Für Unternehmen, Kanzleien oder Praxen ist das schwer planbar.

Managed Services schaffen hier mehr Kalkulationssicherheit:

- **Fixe Monatspauschalen:** Sie zahlen einen fest vereinbarten Betrag und machen Ihre IT-Kosten zu einer verlässlichen Größe in der Budgetplanung.
- **Bedarfsorientierte Modelle:** Sie nutzen genau die Leistungen und Geräte, die Sie tatsächlich benötigen. Wächst Ihr Team, kann der Service flexibel angepasst werden.
- **Weniger Ausfallkosten:** Ein ungeplanter Systemausfall oder ein Sicherheitsvorfall verursacht oft deutlich höhere Kosten als eine kontinuierliche IT-Betreuung.

Mehr Sicherheit bei Datenschutz und IT-Compliance

Mit der Digitalisierung steigen auch die Anforderungen an Datenschutz und IT-Sicherheit. Unternehmen müssen gesetzliche Vorgaben einhalten, Risiken minimieren und gleichzeitig das Vertrauen ihrer Kunden stärken.

Managed Services sorgen dabei für spürbare Entlastung. Sie stellen sicher, dass moderne Sicherheitsstandards und aktuelles Fachwissen kontinuierlich in die Betreuung Ihrer IT einfließen. Dadurch profitieren Sie von einer professionellen, nachhaltigen und zukunftssicheren Umsetzung.

Machen Sie Ihren Job – Ihr IT-Dienstleister übernimmt den Rest

Managed Services sind weit mehr als klassisches Outsourcing. Sie sind ein verlässliches Betreuungskonzept für Unternehmen, die ihre IT stabil, sicher und wirtschaftlich aufstellen möchten. Anstatt Zeit und Energie in unvorhersehbare Störungen, Updates oder Sicherheitsfragen zu investieren, arbeiten Sie mit einer IT-Struktur, die Sie im Alltag unterstützt.

Cyber Risiken besser kontrollieren

Laut Allianz Risk Barometer 2026 sind **Cyber-vorfälle weltweit das Geschäftsrisiko Nr. 1**. Ransomware und andere Cyberangriffe können erhebliche Betriebsunterbrechungen verursachen und neben Reputationsschäden hohe Kosten für Forensik, Wiederherstellung und externe Beratung nach sich ziehen. **Managed Services** können dieses Risiko durch kontinuierliches Monitoring, strukturiertes Patch-Management und schnellere Reaktion **deutlich reduzieren**. Kontaktieren Sie uns.

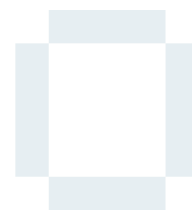
Wissen kompakt!



Proaktiv statt nur im Notfall

Ein wesentlicher Vorteil von Managed Services liegt im proaktiven Ansatz. Probleme werden nicht erst dann bearbeitet, wenn sie bereits den Betrieb beeinträchtigen, sondern möglichst früh erkannt und verhindert.

- > **Reporting:** Monatliche Berichte zeigen Ihnen unter anderem, welche Gefahren abgewehrt und welche Updates durchgeführt wurden.
- > **Verbessern:** Bei Auffälligkeiten oder Fehlern greift Ihr IT-Dienstleister ein und tut alles, um Ihre IT zu optimieren.
- > **Proaktiver Support:** Ihr Dienstleister arbeitet vorausschauend und präventiv, sodass es gar nicht erst zu Problemen kommt.
- > **Fernwartung:** Statt wegen jedes kleinen Problems einen teuren Vor-Ort-Termin zu vereinbaren, bietet Ihr IT-Dienstleister zuverlässige IT-Hilfe aus der Ferne.
- > **Instandhaltung:** Notwendige Aktualisierungen und eine tägliche Systemprüfung sorgen dafür, dass Ihre Geräte stets aktuell bleiben.
- > **Monitoring:** Mit der Dauerbeobachtung überprüft Ihr IT-Dienstleister Prozesse und Vorgänge fortlaufend – und greift im Ernstfall sofort ein.



Basis für flexible und skalierbare Lösungen

Vom virtuellen Lagerraum zur Innovationsplattform: Warum die Cloud für kleine und mittlere Unternehmen längst kein Trend mehr ist, sondern das unverzichtbare Fundament für Wachstum und Sicherheit.

Was ist »die Cloud« eigentlich genau?

Cloud-Computing ist wie ein virtueller Speicherort für Ihre Computerdaten und -programme. Stellen Sie sich vor, Sie könnten all Ihre Unternehmensdaten, Dokumente und Programme nicht auf Ihrem eigenen Computer oder Server speichern, sondern irgendwo im Internet, auf sicheren Servern, die Sie jederzeit von überall aus erreichen können. Das ist die Cloud!

Wie Ihr Unternehmen profitieren kann

Cloud-basierte Systeme sind nicht nur für große Firmen geeignet, sondern auch für kleine Unternehmen. Sie helfen dabei, Geschäftsprozesse einfacher, sicherer und flexibler zu gestalten. Das ist in der heutigen digitalen Welt besonders wichtig.

Ein Beispiel: Anstatt teure Server zu kaufen, können Sie diese in der Cloud mieten. Das spart Geld und Sie müssen sich nicht um die Wartung oder Sicherheit der Server kümmern.

Cloud-Lösungen sind auch bei der Datensicherung äußerst praktisch: Ihre Daten sind sicher, jederzeit verfügbar und werden idealerweise nach strengen deutschen Standards verarbeitet. Zudem sind diese Lösungen oft kostengünstiger, da Sie nur für die tatsächlich genutzten Ressourcen bezahlen (Pay-per-Use).

Cloud-Arbeitsplätze binden Mitarbeiter

Der Vorteil von Cloud-Arbeitsplätzen liegt auf der Hand: Mitarbeiter können dadurch jederzeit und von überall aus

zusammenarbeiten. Falls Sie bisher Bedenken hatten, Homeoffice anzubieten, weil die technischen Voraussetzungen fehlten, ist die Cloud eine gute Lösung.

Die Möglichkeit, von zu Hause aus zu arbeiten, macht Ihr Unternehmen für Mitarbeiter attraktiv und bietet Arbeitsplätze, die den aktuellen Bedürfnissen entsprechen. Außerdem steigert sie die Effizienz und Produktivität, da Mitarbeiter in Echtzeit gemeinsam an Dokumenten, Tabellen und Präsentationen arbeiten können, ohne ständig E-Mails hin- und herschicken zu müssen.

Cloud-Lösungen: Risiken minimieren, Zusammenarbeit verbessern

Die Cloud hilft Ihrem Unternehmen, sich weiterzuentwickeln und gleichzeitig konkurrenzfähig zu bleiben. Indem Sie Daten, Anwendungen und IT-Systeme in sichere Rechenzentren auslagern, reduzieren Sie nicht nur das Risiko von Datenverlusten, sondern sparen auch Geld und Zeit. Außerdem ermöglichen Cloud-Anwendungen Ihren Mitarbeitern, geräte- und standortunabhängig zusammenzuarbeiten.

Warum ist die Cloud besonders gut für kleine Unternehmen?

- > Die Cloud spart Geld und Platz
- > Die Cloud ist flexibel und skalierbar
- > Die Cloud ist sicher und zuverlässig
- > Die Cloud erlaubt Arbeit von überall
- > Die Cloud ermöglicht eine einfache Zusammenarbeit
- > Die Cloud ist immer aktuell

Kurz gesagt!

Wissen kompakt!

Der Cloud-Wegweiser

Public Cloud – die Gemeinschaftliche: Ein Provider stellt Ressourcen über das öffentliche Internet bereit. In dieser Multi-Mandanten-Umgebung teilen sich mehrere Nutzer die physische Infrastruktur des Rechenzentrums. Die Abrechnung erfolgt meist nach tatsächlicher Nutzung.

Private Cloud – die Exklusive: Diese Umgebung ist ausschließlich einem einzigen Unternehmen zugewiesen. Die Infrastruktur wird entweder lokal oder isoliert bei einem Dienstleister betrieben, was volle Kontrolle über Sicherheit und individuelle Konfigurationen ermöglicht.

Hybrid Cloud – die Flexible: Dieser Ansatz verbindet Public- und Private-Umgebungen zu einer integrierten Infrastruktur. Kritische Workloads bleiben im geschützten internen Bereich, während bei Lastspitzen Ressourcen aus der Public Cloud zugeschaltet werden (Cloudbursting).

Multicloud – die Unabhängige: Hier werden gezielt Dienste von zwei oder mehr verschiedenen Cloud-Anbietern parallel genutzt. Das ermöglicht es, für unterschiedliche Aufgaben (z. B. Hosting, Analyse, Sicherheit) jeweils die spezialisierte Technologie verschiedener Provider zu kombinieren.

Bundescloud – die für den Staat: Sie ist die zentrale Betriebsplattform für die IT des Bundes und soll dem hochsicheren Datenaustausch dienen.

Digitale Freiheit für das Handwerk

Die Vision: Standortunabhängigkeit und maximale Ausfallsicherheit

Effizientes Arbeiten – raum- und zeitunabhängig – ist im Zeitalter der Digitalisierung ein zentraler Erfolgsfaktor, gerade für mittelständische Betriebe. Doch oft bremsen veraltete IT-Strukturen diesen Wunsch nach Flexibilität aus.

Genau vor dieser Herausforderung stand ein Elektrobetrieb mit zehn Mitarbeitern. Während die Verwaltung und Disposition die Freiheit des Homeoffice nutzen wollten, suchte der Geschäftsführer nach einem Weg, von jedem Ort aus sicher auf die betriebswirtschaftliche Software zuzugreifen. Die Hürde: Die gesamte IT basierte auf einem lokalen Server, der unter unzureichenden Bedingungen im Lager untergebracht war. Die Folge waren mangelnde Mobilität, Sicherheitsrisiken durch lokale Datenspeicherung auf Einzelrechnern und eine kritisch geringe Ausfallsicherheit.

Die Lösung:

Cloud-Infrastruktur statt Lager-Server

Um die gewünschte Flexibilität zu realisieren, wurde ein Konzept zur vollständigen Migration der On-Premises-Hardware in eine hochverfügbare Cloud-Umgebung umgesetzt. Anstatt in neue, wartungsintensive Hardware vor Ort zu investieren, nutzt der Betrieb nun eine skalierbare Plattform, die mit den Anforderungen mitwächst. Diese Umstellung ermöglicht es zudem, agiler und schneller auf wechselnde Anforderungen im Arbeitsalltag zu reagieren.

Die Vorteile der Cloud-Lösung auf einen Blick:

- > **Grenzenlose Mobilität:** Der Zugriff auf alle Programme ist für das gesamte Team von überall möglich – ob im Büro, auf der Baustelle oder im Homeoffice.
- > **Maximale Resilienz:** Physische Risiken am Standort – wie Stromausfälle, Feuer oder Wasserschäden – werden durch die Cloud-Infrastruktur aufgefangen, sodass sie keine Auswirkungen mehr auf die Datenverfügbarkeit haben.

- > **Zentralisierte Datensicherheit:** Durch die Cloud-Speicherung entfällt die unsichere Datenhaltung auf einzelnen lokalen Rechnern; alle Informationen liegen geschützt an einem zentralen Ort.
- > **Zukunftssichere Skalierbarkeit:** Die IT-Infrastruktur lässt sich jederzeit flexibel an das Wachstum des Unternehmens anpassen.

Projektdynamik:

Herausforderungen erfolgreich meistern

Jeder Technologiewechsel birgt wertvolle Erkenntnisse. Bei der Umstellung von On-Premises auf die Cloud lag das Hauptaugenmerk darauf, Herausforderungen wie die Datenmigration und die Aufrechterhaltung der Geschäftskontinuität souverän zu lösen. Durch eine detaillierte Planung wurde sichergestellt, dass die Ausfallsicherheit während des gesamten Prozesses gewahrt blieb und der tägliche Betrieb unbeeinträchtigt fortgeführt werden konnte.

Das Ergebnis:

Effizienz, die begeistert

Die Erfahrungen des Elektrobetriebs sprechen für sich: Die geplante Flexibilität und Mobilität wurden nachhaltig im Arbeitsalltag verankert. Der Zugriff auf die Software ist ortsunabhängig möglich, was zu einer deutlich gesteigerten Zufriedenheit im Team führt. Der Betrieb ist heute technisch für die Zukunft aufgestellt – mit einer Infrastruktur, die Sicherheit und Freiheit perfekt vereint.





Modern Workplace

Modern Workplace, digitaler Arbeitsplatz, Arbeitsplatz der Zukunft – die Bezeichnungen sind so vielfältig wie das Verständnis darüber, was modernes Arbeiten ausmacht. Doch was steckt wirklich dahinter? Ein neues Gerät allein macht noch keinen Modern Workplace. Technologie ermöglicht moderne Arbeit, ist jedoch nur ein Teil der Lösung.

Mehr als ein Schreibtisch

Unter einem Modern Workplace versteht man das Zusammenspiel von Geräten, Software und Prozessen – konsequent ausgerichtet auf die Anforderungen Ihrer Mitarbeiter. Im Mittelpunkt steht das Team: Ziel ist flexibles, vernetztes Arbeiten – unabhängig von Ort und fester Präsenzzeit. Damit dieser Wandel gelingt, ist ein Umdenken erforderlich: Moderne Arbeit orientiert sich am Bedarf – nicht dem Standort. Wer Fachkräfte gewinnen und binden will, muss Erwartungen wie Homeoffice und reibungslose digitale Abläufe erfüllen. Dafür braucht es ein Konzept, das Infrastruktur, Anforderungen der Fachbereiche und IT-Sicherheit zusammenführt. Verbindliche Standards sorgen dafür, dass digitale Werkzeuge im Arbeitsalltag zuverlässig funktionieren. Um dieses Konzept umzusetzen, stützt sich der Modern Workplace auf vier zentrale Säulen:

Die vier Säulen des modernen Arbeitens

Produktivität durch KI

KI kann als digitaler Assistent Routineaufgaben reduzieren, Informationen schneller auffindbar machen und wiederkehrende Arbeitsschritte vereinfachen. Das schafft Freiraum für Aufgaben, die Erfahrung und Urteilskraft erfordern.

Nahtlose Zusammenarbeit

Zusammenarbeit sollte sich selbstverständlich anfühlen. Gemeinsames Bearbeiten von Dokumenten, Meetings, Chat und Aufgabenmanagement greifen ineinander. So sinken Reibungsverluste und Abstimmungen werden schneller.

Grenzenlose Mobilität

Arbeit ist eine Tätigkeit, kein Ort. Ein moderner Arbeitsplatz funktioniert überall dort, wo das Internet verfügbar ist – und auf den relevanten Endgeräten. Ob Datenzugriff oder Telefonie: Die Arbeitsumgebung folgt dem Nutzer vom Laptop bis zum Smartphone.

Intelligente Sicherheit

Mit mehr Flexibilität wächst die Angriffsfläche. Da Zugriffe von überall erfolgen, bilden Identitätsschutz, Multi-Faktor-Authentifizierung und Verschlüsselung das Fundament. IT-Sicherheit ist kein Extra, sondern Voraussetzung für Stabilität.

Warum moderne Arbeitswelten den Unterschied machen

Die Umstellung auf einen Modern Workplace ist kein reines IT-Update. Sie macht Arbeitsabläufe verlässlicher und reduziert Reibung im Tagesgeschäft. Drei Vorteile fallen in KMU besonders schnell auf:

Vorsprung im Recruiting

Viele Fachkräfte erwarten flexible Arbeitsmodelle und zeitgemäße Tools. Ein Modern Workplace liefert dafür die Basis. Er zeigt, dass mobiles Arbeiten, Zusammenarbeit und Support nicht dem Zufall überlassen sind.

Höhere Effizienz, weniger Reibung

Wenn Arbeitswege klar sind, sinken Suchzeiten und Doppelarbeit. Teams arbeiten seltener mit falschen Versionen. Entscheidungen bleiben nachvollziehbar und Übergaben funktionieren besser.

Krisenfestigkeit und Skalierbarkeit

Ein digitales Fundament ermöglicht es, schnell auf Veränderungen zu reagieren. Kurzfristiges Homeoffice, neue Standorte oder zusätzliche Mitarbeiter lassen sich planbarer umsetzen. Standardisiertes Onboarding und zentrale Richtlinien sorgen für stabile Abläufe.

Strategie in der Praxis

Da der Modern Workplace kein starres Produkt ist, sondern eine Strategie, zeigt er sich in der Praxis durch verschiedene Arbeitsmodelle und technologische Konzepte:

1. Organisatorische Ebene

Arbeitsmodelle

Diese Ebene beschreibt, wie und wo Zusammenarbeit stattfindet:

> Hybrid Work

Eine verbreitete Form. Mitarbeiter teilen ihre Zeit zwischen Büro und Homeoffice. Die Herausforderung ist die »Synchronisation« – besteht also darin, Kommunikation und Entscheidungen für alle gleichermaßen zugänglich zu halten.

> Remote-First

Büros gibt es oft noch, der Standardprozess ist jedoch auf Distanz ausgelegt. Meetings sind grundsätzlich virtuell organisiert, damit niemand benachteiligt wird.

> Aufgabenbezogenes Arbeiten

Im Büro gibt es keine festen Schreibtische. Mitarbeiter wählen den Platz passend zur Aufgabe: Fokus-Raum für Konzentration, offene Bereiche für Austausch oder Konferenzräume für hybride Meetings.

2. Technische Ebene

Bereitstellung

Diese Ebene beschreibt, womit gearbeitet wird und wie die IT-Umgebung strukturiert ist:

> Cloud-Native Workplace

Anwendungen laufen im Browser oder über Apps. In vielen Szenarien wird VPN entbehrlich, wenn Sicherheit über Identität, Gerätestatus und Richtlinien gesteuert wird (Zero Trust).

> Virtual Desktop Infrastructure (VDI)/Cloud PC

Das Betriebssystem wird zentral auf Servern betrieben. Der Desktop wird auf das Endgerät übertragen. Vorteil: geringeres Datenabflussrisiko, weil Daten überwiegend zentral bleiben.

> Bring Your Own Device (BYOD) vs. Choose Your Own Device (CYOD)

Bei BYOD nutzen Mitarbeiter private Geräte (erfordert striktes Mobile Device Management). Bei CYOD stellt das Unternehmen einen Gerätekatalog bereit. Das vereinfacht Support und Standards, ohne Wahlfreiheit komplett zu verlieren.

3. Physische Ebene

Smart Office

Das Smart Office ist die physische Hülle des Modern Workplace. Hier wird das Gebäude selbst zum digitalen Werkzeug:

> IoT-gestützte Arbeitsplätze

Sensoren zeigen in Echtzeit, welche Plätze verfügbar sind.

> Hybride Hubs

Räume mit guter Audio-/Video-Technik und digitalen Whiteboards unterstützen hybride Zusammenarbeit, ohne Medienbrüche.



IT-Sicherheit als Grundpfeiler der Digitalisierung

Ob mobile Zeiterfassung im Handwerk, vernetzte Produktionsanlagen in der Industrie oder hybride Arbeitsmodelle im Dienstleistungssektor: Digitale Prozesse machen Betriebe schneller, flexibler und effizienter. Doch jeder Motor braucht ein stabiles Gehäuse, das ihn schützt. Genau diese Rolle übernimmt die IT-Sicherheit.

Ohne Sicherheit keine Digitalisierung

Oft wird die Bedeutung von IT-Sicherheit erst sichtbar, wenn es zu spät ist: wenn Systeme ausfallen, Daten verschlüsselt werden oder ein einziger Klick eine Kettenreaktion auslöst. Dann zeigt sich, dass Digitalisierung nur so stark ist wie die Sicherheit, auf der sie aufbaut. IT-Sicherheit ist deshalb nicht bloß Begleitschutz – sie ist die Voraussetzung dafür, dass digitale Innovation im Alltag überhaupt zuverlässig funktionieren kann.

Das Ende der Burggraben-Mentalität

Lange Zeit funktionierte IT-Sicherheit nach einem einfachen Bild: Unternehmen bauten eine Burg. Außen schützte eine starke Mauer, davor lag der Burggraben in Form einer Firewall. Wer einmal drinnen war, galt als vertrauenswürdig. Dieses Modell war übersichtlich – und in einer weniger vernetzten Welt oft ausreichend.

Heute aber hat die Burg längst mehr Tore, Nebeneingänge und Zugbrücken als früher. Mitarbeiter arbeiten im Homeoffice, greifen unterwegs über Tablets und Smartphones auf Systeme zu und nutzen Cloud-Dienste, die weit außerhalb der alten Mauern liegen. Die Folge: Die Angriffsfläche wächst. Und Angreifer müssen die Burg nicht mehr frontal stürmen – oft reicht eine täuschend echte Phishing-Mail, um die Tür von innen öffnen zu lassen.

Genau deshalb reicht es nicht mehr, nur die Außenmauer zu verstärken. Moderne IT-Sicherheit verbindet Technik und Mensch. Die Technik spannt den Schutzschirm auf, doch die Mitarbeiter bleiben ein entscheidender Teil der Verteidigung. Sie sind die »Human Firewall«, das menschliche Schutzschild, die verdächtige Signale erkennt, aufmerksam bleibt und Angriffe nicht ungewollt ins Unternehmen hineinträgt.

Sicherheit beginnt also nicht erst im Serverraum, sondern im Verhalten und Bewusstsein der Menschen. (Lesen Sie mehr dazu auf der nächsten Doppelseite.)

Sicherheit ohne Blindvertrauen

Wenn die Grenzen zwischen innen und außen verschwimmen, braucht es ein neues Sicherheitsprinzip. Dieses Prinzip heißt Zero Trust. Dahinter steckt ein einfacher, aber wirkungsvoller Gedanke: Vertrauen wird nicht pauschal vergeben. Jede Anfrage, jeder Zugriff und jedes Gerät müssen sich immer wieder neu legitimieren – unabhängig davon, ob der Zugriff aus dem Büro, aus dem Homeoffice oder von der Baustelle erfolgt.

Das ist ein grundlegender Perspektivwechsel. Statt zu sagen »Wer drinnen ist, gehört dazu«, gilt nun: »Vertrauen muss jederzeit überprüft werden.« Mitarbeiter erhalten nur die Zugriffsrechte, die sie für ihre konkrete Aufgabe tatsächlich brauchen. Dieses Prinzip der minimalen Rechtevergabe – Least Privilege – sorgt dafür, dass aus einem gestohlenen Passwort nicht automatisch ein Generalschlüssel für das gesamte Unternehmen wird.

Selbst wenn ein Angreifer an einer Stelle eindringt, stößt er nicht auf offene Flure, sondern auf verschlossene Türen. So verhindert Zero Trust, dass sich ein Sicherheitsvorfall unbemerkt durchs gesamte Netzwerk frisst. Das Unternehmen bleibt beweglich, ohne sich schutzlos zu machen.

Von der Abwehr zur Widerstandskraft

Doch selbst die beste Verteidigung kann nicht garantieren, dass niemals etwas passiert. Entscheidend ist deshalb nicht nur, ob ein Angriff abgewehrt wird, sondern auch, wie gut ein Unternehmen mit dem Ernstfall umgehen kann. Genau hier kommt Cyber-Resilienz ins Spiel.

Während Cybersicherheit darauf zielt, Angriffe zu verhindern, geht Cyber-Resilienz einen Schritt weiter: Sie sorgt dafür, dass ein Unternehmen auch dann handlungsfähig bleibt, wenn ein Angriff erfolgreich gewesen ist. Es geht also nicht nur darum, den Einschlag zu vermeiden, sondern darum, nach einem Treffer nicht auseinanderzubrechen.

Ein resilientes Unternehmen ist darauf vorbereitet, Störungen auszuhalten, Schäden zu begrenzen und den Betrieb schnell wieder aufzunehmen. Nicht Panik, sondern Reaktionsfähigkeit wird zum Maßstab. Aus einem potenziell existenzbedrohenden Vorfall wird so ein beherrschbarer Zwischenfall.

Vier Bausteine einer widerstandsfähigen Sicherheitsstrategie

Damit diese Widerstandskraft nicht nur auf dem Papier besteht, braucht es vier eng verzahnte Bausteine:

1. Transparenz und Endpunkt-Verwaltung

Wer sich schützen will, muss seine eigene IT-Landschaft kennen. Unternehmen müssen wissen, welche Geräte, Anwendungen und Systeme überhaupt im Einsatz sind – vom Laptop über das Smartphone bis zum Server. Nur mit dieser Sichtbarkeit lassen sich Auffälligkeiten erkennen, bevor sie zum Problem werden.

2. Kontinuierliche Kontrollhygiene

Sicherheit ist kein Zustand, den man einmal erreicht und dann abhakt. Im Alltag verrutschen Einstellungen, Schutzfunktionen werden deaktiviert oder Updates verändern Konfigurationen. Kontrollhygiene bedeutet, regelmäßig zu prüfen, ob alle Schutzmechanismen weiterhin korrekt eingerichtet sind – und auch tatsächlich funktionieren.

3. Zero Trust Network Access (ZTNA)

ZTNA bringt das Zero-Trust-Prinzip in die Praxis. Jeder Zugriff

auf Anwendungen und Systeme wird in Echtzeit geprüft. So wird verhindert, dass ein kompromittiertes Konto sich wie ein Brandherd durchs Unternehmen ausbreitet. Der Schaden bleibt lokal begrenzt, statt den ganzen Betrieb lahmzulegen.

4. Schnelle Wiederherstellung und kontinuierliches Lernen

Wenn der Ernstfall eintritt, zählt jede Minute. Dann braucht es mehr als nur Datensicherungen. Gefragt sind klare Abläufe, definierte Verantwortlichkeiten und ein abgestimmtes Zusammenspiel zwischen IT, Fachbereichen und Geschäftsführung. Ebenso wichtig ist die Analyse des Vorfalls: Was ist passiert, warum konnte es passieren und wie lässt sich die Verteidigung künftig stärken? Resilienz heißt auch, aus Angriffen zu lernen.

Sicherheit als strategischer Vorsprung

IT-Sicherheit ist kein Bremsklotz der Digitalisierung. Sie ist das, was ihr Stabilität, Richtung und Verlässlichkeit gibt. Sie schützt nicht nur Daten und Systeme, sondern auch das Vertrauen von Kunden, Partnern und Mitarbeitern.

In einer Wirtschaft, in der digitale Ausfälle schnell teuer und imageschädigend werden können, ist Widerstandskraft ein echter Wettbewerbsvorteil. Wer heute in moderne Sicherheitskonzepte, geschulte Mitarbeiter und resiliente Strukturen investiert, schützt sein Unternehmen nicht nur vor Risiken – er schafft die Grundlage für nachhaltiges Wachstum. So wird IT-Sicherheit vom reinen Schutzmechanismus zum strategischen Erfolgsfaktor der digitalen Zukunft.

Selbsttest

Sind die Zugänge von Mitarbeitern, die das Unternehmen im vergangenen halben Jahr verlassen haben, wirklich in allen Systemen und Cloud-Diensten gelöscht?

☐☐

Gibt es einen Notfallplan in der Schublade, der beschreibt, was zu tun ist, wenn morgen früh kein PC mehr hochfährt?

☐☐

Ist von jedem Gerät im Homeoffice bekannt, ob der Virenschutz aktiv und aktuell ist?

☐☐

Beim »Nein« ertappt?

Keine Sorge, Sie sind nicht allein. IT-Sicherheit und Resilienz sind keine Zustände, die man von heute auf morgen »erledigt«. Es sind Prozesse. Der erste Schritt ist die Erkenntnis, zu wissen, wo die Lücken liegen. Der zweite Schritt ist ein starker Partner an Ihrer Seite, der Technik, Mensch und Strategie zu einem echten Grundpfeiler verbindet. Kontaktieren Sie uns.



Digitale Skills für den Wandel



Die Rolle der Mitarbeiter

Digitalisierung birgt große Potenziale, doch gleichzeitig begünstigt sie raffiniertere Cyberangriffe. Da Geschäftsprozesse, Kommunikation und sensible Daten zunehmend ins Netz verlagert werden, wächst die digitale Angriffsfläche stetig. Neben Technik rückt ein Faktor besonders in den Fokus von Cyberkriminellen: der Mensch.

Die Evolution der Gefahr: Phishing im KI-Zeitalter

Phishing beschreibt das »Angeln« nach Zugangsdaten oder vertraulichen Informationen. Angriffe erfolgen über E-Mails, gefälschte Websites oder täuschend echte Profile. Es ist längst kein plumpes Massenphänomen mit offensichtlichen Rechtschreibfehlern mehr, sondern eine Form des Social Engineering – der gezielten sozialen Manipulation. Mit generativer Künstlicher Intelligenz hat diese Bedrohung an Qualität gewonnen.

KI-gestützte Phishing-E-Mails wirken oft sehr überzeugend. Sie imitieren Sprache, Tonalität und Stil echter Geschäftskorrespondenz. Statt auf auffällige Anhänge zu setzen, die Filter abfangen könnten, zielen moderne Angriffe häufig auf:

- > **Emotionale Trigger:**
Angst, Neugier oder Hilfsbereitschaft.
- > **Kontextbezug:**
Bezug auf Projekte, Rollen oder reale Ansprechpartner.
- > **Druck und Autorität:**
»Sofort handeln«, »vertraulich«, »Chef-Anweisung«.

Selbst geschulte Mitarbeiter erkennen solche Nachrichten nicht immer auf den ersten Blick. Gelingt der Einstieg, versuchen Angreifer häufig, sich unauffällig im Netzwerk weiterzubewegen. Dafür nutzen sie nicht selten vorhandene, legitime Werkzeuge.



Technik allein ist kein Allheilmittel

Moderne, KI-basierte Abwehrsysteme erkennen viele Anomalien automatisch und melden Verdachtsfälle. Sie analysieren Muster, Abweichungen und ungewöhnliche Zugriffe. Trotzdem bleibt ein kritischer Moment: die menschliche Entscheidung. Ein Klick, eine Freigabe oder die Eingabe von Zugangsdaten kann ausreichen.

Deshalb wandelt sich die Rolle der Belegschaft: Aus einem potenziellen Risiko wird ein aktiver Schutzfaktor. Dafür braucht es konkrete Fähigkeiten, die im Alltag greifen.

Die entscheidenden »Digital Skills« für den Wandel

Um in der modernen Arbeitswelt sicher zu agieren, benötigen Mitarbeiter mehr als nur IT-Grundkenntnisse. Drei Fähigkeiten sind besonders relevant:

1. Quellenkritik und kontextuelle Intuition

Mitarbeiter sollten Informationen kritisch hinterfragen und einordnen. Passt eine Zahlungsaufforderung zum Prozess? Ist der genutzte Kommunikationskanal üblich? Stimmt die Absenderadresse? Kleine Abweichungen sind oft entscheidend.

2. Psychologische Resilienz

Social Engineering nutzt Stress. Ein zentraler Skill ist das Innehalten bei »Dringend«-Situationen. Klare Regeln helfen: Rückruf über bekannte Nummern, Vier-Augen-Prinzip bei Zahlungen, Rückfrage im Team statt schnelle Reaktion.

3. Digitale Selbstverteidigung

Multi-Faktor-Authentifizierung, Passwortmanager und sichere Identitäten müssen Routine sein. Dazu gehört auch: Updates akzeptieren, Geräte sperren, keine privaten Umgehungs-lösungen nutzen. So sinkt das Risiko bei Kontoübernahmen.

Von der Schulung zur gelebten Sicherheitskultur

Ein Vortrag pro Jahr reicht nicht. Wirksame Awareness ist praxisnah und wiederholbar:

- > **Realitätsnahe Simulationen:** Regelmäßige, unangekündigte Phishing-Tests schärfen die Aufmerksamkeit im Arbeitsalltag.
- > **Offene Fehlerkultur:** Mitarbeiter müssen sich trauen, Verdachtsfälle oder Fehlritte sofort zu melden, ohne Sanktionen zu befürchten.
- > **Dynamische Anpassung:** Da sich Methoden laufend ändern, muss auch der Wissensaufbau kontinuierlich erfolgen.

Moderne Sicherheitstechnologien bilden das Fundament. Doch Wachsamkeit und Sicherheitsverhalten im Team entscheiden über die Wirksamkeit der Verteidigung. Eine aufmerksame Belegschaft ist eine der stärksten Schutzmaßnahmen, die ein Unternehmen im digitalen Wandel etablieren kann. Wir unterstützen Sie dabei, diese proaktive Schutzmauer aufzubauen – sowohl auf der technischen Ebene durch moderne Abwehrsysteme als auch auf der menschlichen Ebene durch zielgerichtete Awareness-Trainings.



> Der menschliche Faktor

Was den ganzheitlichen Schutz vor Social Engineering unmöglich macht, ist, dass wir als Menschen nur perspektivisch wahrnehmen können und damit Informationen verborgen bleiben. Private oder berufliche Interaktionen entstehen aus subjektiven Gedanken und Gefühlen sowie aus objektiven Annahmen und daraus resultierenden Entscheidungen. Dieses Phänomen wird »menschlicher Faktor« genannt.

> Die »Schwachstelle Mensch«

Der menschliche Faktor wird dann zur »Schwachstelle«, wenn er von bestimmten Personen oder Gruppen erkannt und gezielt ausgenutzt wird. Dies passiert beim Social Engineering. Dabei werden Vertrauen sowie offengelegte Angst, Hoffnung, Hilfsbereitschaft, Neugierde und autoritärer Gehorsam genutzt, um Menschen zum gewünschten Handeln zu bewegen. Vor allem, wenn etwas Unerwartetes passiert und in Krisen- und Stresssituationen, tendieren Menschen dazu, irrational zu handeln und sich manipulieren zu lassen.

Kurz gesagt!

Selbsttest

Ja Nein

Haben Sie in letzter Zeit unangekündigt getestet, ob Ihre Mitarbeiter auf eine fingierte Phishing-E-Mail klicken würden?

☐☐

Wissen Ihre Mitarbeiter, an wen sie sich innerhalb von 60 Sekunden wenden müssen, wenn sie glauben, gerade auf einen schädlichen Link geklickt zu haben – ohne Angst vor Ärger?

☐☐

Ist es in Ihrem Unternehmen verboten, private USB-Sticks oder eigene Cloud-Speicher für Firmendaten zu verwenden, weil die internen Lösungen zu kompliziert sind?

☐☐

Beim »Nein« ertappt?

Keine Sorge, Sie sind nicht allein. Der erste Schritt ist zu erkennen, wo die Lücken liegen. Der zweite Schritt ist ein starker Partner an Ihrer Seite, der Technik, Mensch und Strategie zu einem echten Grundpfeiler verbindet. Kontaktieren Sie uns.



Grüne IT für KMU

Die Digitalisierung schreitet rasant voran und mit ihr der Hunger nach Rechenleistung. Was viele Nutzer im Alltag kaum wahrnehmen: Hinter jedem Klick, jeder E-Mail, jeder Eingabe in eine KI und jedem Videocall verbirgt sich ein realer Bedarf an Rohstoffen und Energie.

Aber: Die Digitalisierung als Klimaretter statt als Klimakiller – dieser Hoffnung machende Rollentausch findet im Green-IT-Ansatz seinen Ausdruck.

Ein ganzheitlicher Ansatz

Green IT, auch nachhaltige IT genannt, bezeichnet das Ziel, Informations- und Kommunikationstechnik über den gesamten Lebenszyklus umweltverträglich zu gestalten. Entscheidend sind drei Punkte: verantwortungsvolle Herstellung, energieeffizienter Betrieb und fachgerechte Wiederverwendung oder Entsorgung. So sinken Ressourcenverbrauch und Emissionen, ohne die Leistungsfähigkeit Ihrer IT zu gefährden.

Für KMU bedeutet das zwei Hebel:

- **Green in IT:** Sie reduzieren den ökologischen Fußabdruck Ihrer IT. Das gelingt durch langlebige Geräte, passende Leistungsprofile und konsequentes Energiemanagement. Auch Virtualisierung und ein sauber geplantes Geräteleben verlängern Nutzungszeiten.
- **Green by IT:** Sie nutzen Digitalisierung, um Emissionen in Geschäftsprozessen zu senken. Videokonferenzen ersetzen viele Reisen. Digitale Workflows sparen Papier und Transporte. Sensorik und Auswertungen helfen, Energie in Gebäuden bedarfsgerecht zu steuern.



Bits, Bytes & grüne Bilanz:

Wie KMU die Digitalisierung nachhaltig gestalten

Vom Einkauf bis zum Kreislauf

Nachhaltigkeit beginnt vor dem ersten Einschalten. Eine bewusste Beschaffung priorisiert langlebige Hardware mit Umweltlabels und reparaturfreundlicher Architektur. Einheitliche Modelle und lange Update-Zyklen reduzieren nicht nur Elektroschrott, sondern vereinfachen auch die Wartung. Den Abschluss bildet eine echte Kreislaufwirtschaft: Nachweisbare Datenlöschung gefolgt von professionellem Refurbishing oder fachgerechtem Recycling.

Datenhygiene und intelligente Infrastruktur

Hardware ist nur so effizient wie die darauf laufenden Prozesse. »Cyber-Müll« – also ungenutzte Datenbestände und Dubletten – ist ein stiller Energiefresser; konsequente Datenhygiene daher aktiver Klimaschutz. Im Serverraum bietet die Virtualisierung das größte Potenzial: Durch die Bündelung mehrerer Systeme auf minimaler Hardware sinken Strombedarf und Kühlaufwand bei steigender Ausfallsicherheit.

Effizienz durch Cloud und KI

Professionelle Rechenzentren nutzen Skaleneffekte sowie optimierte Kühlung und arbeiten meist effizienter als lokale Lösungen. Entscheidend ist die Transparenz: Ein Wechsel lohnt sich ökologisch vor allem bei Providern, die nachweislich auf erneuerbare Energien setzen. Künstliche Intelligenz agiert dabei als Doppelagent: Während das Training Ressourcen bindet, fungiert sie im Betrieb als Effizienz-Turbo. Richtig konfiguriert, optimiert KI Lastverläufe in Echtzeit und verhindert Energieverschwendung durch Leerlauf oder Fehlbetriebe. Es gilt: So viel KI wie nötig, so ressourcenschonend wie möglich.

Messbarkeit schafft Transparenz

Monitoring macht Green IT von der Absicht zur messbaren Realität. Erst wenn der Verbrauch je Gerätegruppe transparent ist, lassen sich Grenzwerte definieren und Erfolge kontrollieren. So wird IT-Effizienz zur betriebswirtschaftlichen Kennzahl, die direkt auf die Wirtschaftlichkeit einzahlt.



Checkliste

Handeln statt Abwarten – Ihr Fahrplan für eine grüne IT

Nachhaltigkeit in der IT ist kein monumentales Projekt, sondern ein Prozess aus vielen klugen Entscheidungen. Unsere Checkliste zeigt Ihnen, wo Sie sofort ansetzen können, um Kosten zu senken und Ressourcen zu schonen.

Sofortmaßnahmen für den Arbeitsalltag

- ☐ **Standby-Stopp:** Automatische Abschaltung für PCs, Monitore und Drucker nach Feierabend einrichten.
- ☐ **Effizienz-Profil:** Display-Abschaltung und CPU-Drosselung zentral per Richtlinie steuern.
- ☐ **Digital-First:** Standardmäßig »beidseitig« und »Schwarzweiß« drucken; digitale Freigaben bevorzugen.

Infrastruktur & Technologie

- ☐ **Virtualisierung:** Systeme bündeln, um physische Server und Kühlaufwand zu reduzieren.
- ☐ **Cloud-Check:** Workloads nur an Provider mit transparentem Ökostrom-Nachweis auslagern.
- ☐ **KI-Einsatz:** Fokus auf Anomalie-Erkennung und Wartungsplanung zur Vermeidung von Fehlbetrieb.

Beschaffung & Datenhygiene

- ☐ **Second Life:** Professionell aufbereitete Business-Geräte (Refurbished) in die Planung einbeziehen.
- ☐ **Daten-Frühjahrsputz:** Duplikate löschen und feste Archivierungsregeln für Schattenablagen einführen.
- ☐ **Label-Pflicht:** Energy Star, EPEAT oder Blauer Engel als feste Kriterien für den Einkauf definieren.

Monitoring & Entsorgung

- ☐ **Verbrauchsmessung:** Strombedarf je Gerätegruppe erfassen und »Dauerläufer« identifizieren.
- ☐ **Klima-Check:** Serverraum-Temperatur moderat anheben und Luftführung optimieren.
- ☐ **Sicheres Recycling:** Nachweisbare Datenlöschung sicherstellen; Rücknahmesysteme für Toner und Akkus nutzen.

Durch eine strukturierte IT-Modernisierung sinken nicht nur Ihre laufenden Kosten – auch Ihr ökologischer Fußabdruck wird deutlich reduziert. Sichern Sie sich so einen klaren Wettbewerbsvorteil und stärken das Vertrauen bei Kunden und Investoren. Nehmen Sie gern Kontakt zu uns auf und informieren Sie sich über nachhaltige IT-Lösungen.



Wissen kompakt!

Das KI-Paradoxon

KI treibt die Digitalisierung, fordert aber gewaltige Ressourcen: Neben Strom aus größtenteils fossilen Quellen ist vor allem der Wasserbedarf zur Kühlung kritisch. Laut Gesellschaft für Informatik benötigt ein durchschnittliches deutsches Rechenzentrum täglich bis zu 1,8 Millionen Liter Wasser; bis 2030 könnte der landesweite Bedarf auf 240 Milliarden Liter pro Jahr steigen. Parallel dazu prognostiziert die Internationale Energieagentur einen weltweiten Strombedarf von 945 Terawattstunden – eine Dimension, die dem Jahresbedarf Japans entspricht. Vor allem

das Training generativer Modelle beschleunigt diesen Trend.

Die Technologie als Lösung: In der Praxis hilft KI bereits heute, Emissionen aktiv zu senken. Intelligente Algorithmen optimieren Kühlsysteme in Echtzeit oder verschieben rechenintensive Prozesse automatisch in Zeitfenster mit hohem Ökostrom-Angebot. Über den betrieblichen Nutzen hinaus unterstützt KI zudem globale Forschungsprojekte bei zukunftsweisenden Klimaschutz-Anwendungen.



Überreicht durch:

Schempp Networks

Hugenottenallee 51 | 63263 Neu-Isenburg

Tel. +49 6102 7192980 | office@schempp-networks.de

www.schempp-networks.de

