Die Rolle von IT-Leitern in Zeiten von AI

Schatten-IT, Sicherheitsrisiken & IT-Overload – Wie HP AI-Notebooks IT-Leiter:innen bei täglichen Herausforderungen entlasten.

IT-Abteilungen stehen vor einem doppelten Dilemma: Einerseits steigen Komplexität, Sicherheitsrisiken und Verwaltungsaufwand. Andererseits erwarten Geschäftsführung und Mitarbeitende flexible, moderne Arbeitsumgebungen – mit minimaler IT-Abhängigkeit. Datengestützte Entscheidungen sollen möglichst in Echtzeit getroffen werden. Der Einsatz generativer AI nimmt in diesen Prozessen rapide zu – und damit auch die Risiken.

Der Siegeszug der AI sorgt in vielen IT-Abteilungen für große Probleme. Schatten-IT, veraltete Endgeräte und Fachkräftemangel verschärfen diesen Zielkonflikt täglich. Während Mitarbeitende längst eigene AI-Tools im Arbeitsalltag nutzen, fehlt es in vielen Unternehmen an einer einheitlichen Strategie, wie neue Technologien sicher, effizient und standardisiert eingeführt werden können.

Zahlen belegen den Handlungsdruck:

75%

der Mitarbeiter nutzen bereits AI bei der Arbeit.

Quelle: Microsoft Copilot+ Studie

78%

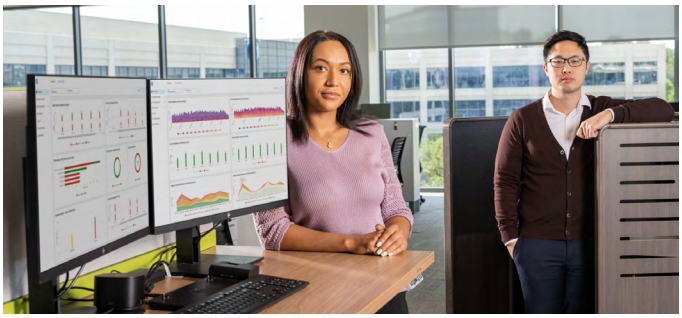
bringen eigene AI-Tools mit zur Arbeit (BYOAI)

Quelle: Microsoft BYOAI Insight – 'Bring Your Own AI' Report

52%

verschweigen ihre AI-Nutzung

Quelle: Microsoft Copilot+ Studie / Work Trend Index



Zahlreiche solcher Anwendungen werden ohne Wissen und Genehmigung des Unternehmens, geschweige denn der IT-Abteilung, genutzt. Viele Mitarbeitende setzen auf eigene AI-Tools anstatt auf solche, die vom Unternehmen bereitgestellt werden – ein Trend, den Microsoft „BYOAI" („Bring Your Own AI") nennt.

Eine Umfrage von Microsoft hat ergeben, dass rund 52 % der Mitarbeiter in mittelständischen Unternehmen und Konzernen den Einsatz der AI-Tools verschweigen.

Die Gründe dafür sind ganz einfach: Das unautorisierte Nutzen zeigt den starken Wunsch nach künstlicher Intelligenz und das Interesse an schnellen, einfachen und besseren Arbeitsergebnissen. Auf der anderen Seite zeigt das Ergebnis die große Angst der Arbeitnehmer, ersetzbar zu sein. Besonders niedrige Einkommensgruppen und Frauen blicken mit Sorgen auf die Entwicklung von AI.

Auch viele Studenten blicken heute bereits skeptisch auf ihre berufliche Zukunft. Die Angst besteht, dass es den erlernten Beruf in wenigen Jahren noch gibt. Unternehmen, die von AI profitieren wollen, sollten daher die Nutzung durch Mitarbeiter positiv hervorheben und Schulungen anbieten.

Was IT jetzt braucht: Smart Governance

Patchen, Absichern, Firefighting – statt Zukunft gestalten. So sieht der Alltag in vielen IT-Abteilungen auf der gesamten Welt aus. Veraltete PC-Flotten werden somit zum stillen Kostenfaktor in Unternehmen. Weltweit sind noch über 237 Millionen Windows-10-Geräte aktiv. Diese sind älter als vier Jahre und bekommen ab Oktober 2025 keine Sicherheitsupdates mehr – sie werden somit zu einem offenen Scheunentor für Angreifer.

Die Antwort liegt also auf der Device-Ebene: Smart Governance. Governance bedeutet Kontrolle. Aber nicht durch Einschränkung – sondern durch Struktur, Voraussicht und Automatisierung. IT darf nicht mehr nur reagieren, sondern muss aktiv vorstrukturieren – mit standardisierten, AI-fähigen Devices. Genau das ermöglichen AI-PCs wie das HP EliteBook Ultra G1i. HP AI-Notebooks sind keine Laptops. Sie sind Governance-Werkzeuge. Sie sind ideal für hybride Arbeitsmodelle und ermöglichen effiziente Rollouts, klare Rechtevergabe und sorgen für geringen Support.

Vier Säulen smarter IT-Governance mit HP AI-PCs

Einheitliche Geräteflotte statt IT-Wildwuchs

Sicherheit ab Werk – tief im Gerät verankert

Lokale AI statt Schatten-Clouds

Automatisierte IT-Entlastung via HP TechPulse

HP Wolf Security for Business: Maximale Sicherheit – dort, wo andere Lösungen nicht greifen

Maximale Sicherheit für Ihre IT

Moderne Bedrohungsszenarien zielen längst unterhalb des Betriebssystems auf Firmware, BIOS und Identitätsdaten.

HP Wolf Security begegnet diesen Angriffsmustern mit einer hardwaregestützten Architektur: Isolierte Mikro-VMs (Virtuelle Maschinen) verhindern, dass Schadsoftware auf das System zugreift. Angriffe werden automatisch erkannt und gekapselt, bevor sie sich ausbreiten.

Sollte dennoch eine Manipulation am BIOS erfolgen, setzt sich das System durch das Self-Healing-BIOS selbstständig auf einen intakten Zustand zurück.

Diese Wiederherstellungsfähigkeit sichert nicht nur die Betriebsfähigkeit – sie verhindert auch nachhaltige Kompromittierungen.

HP Wolf Security ist damit kein Add-on, sondern eine tief integrierte Sicherheitsinfrastruktur auf Enterprise-Niveau. Besonders in Umgebungen mit verteilten Arbeitsplätzen und mobilen Endgeräten ist diese Schutzwirkung essenziell, um IT-Risiken wirksam zu minimieren.

66 Mio.

Business-Email-Compromise-Angriffe pro Monat weltweit – oft AI-generiert.

Quelle: HP AI Security Slides / Microsoft Angabe

HP TechPulse: Remote Management und vorausschauende Entlastung

Die Anforderungen an IT-Abteilungen wachsen – die Personaldecke nicht. Mit HP TechPulse erhalten Unternehmen eine cloudbasierte Plattform zur Fernüberwachung und vorausschauenden Steuerung der gesamten Geräteflotte. Sensorbasierte Telemetriedaten liefern frühzeitig Hinweise auf mögliche Ausfälle, Softwarekonflikte oder Sicherheitslücken. Updates, Patches und Konfigurationen lassen sich zentral automatisieren – ganz ohne manuelle Eingriffe vor Ort. Für IT-Teams bedeutet das: weniger Routineaufgaben, weniger Eskalationen, weniger Stillstand. Für das Unternehmen: maximale Geräteverfügbarkeit, bessere Planbarkeit und deutlich geringerer Aufwand im Lifecycle-Management.

Microsoft Pluton & AI-Security: Schutz beginnt in der CPU

Viele Sicherheitslösungen setzen zu spät an. Microsoft Pluton geht einen anderen Weg: Der Sicherheitsprozessor ist direkt in die CPU des Geräts integriert und schützt die digitalen Identitäten und Zugriffsrechte bereits auf der untersten Hardwareebene. Angreifer können damit weder über physische noch über virtuelle Wege auf Credential-Daten zugreifen – selbst wenn sie tiefen Systemzugriff erlangen. Ergänzt wird diese Architektur durch AI-gestützte Mechanismen zur Anomalieerkennung und Zugriffskontrolle. Das Ergebnis ist ein Schutzmodell, das Angriffe nicht nur blockiert, sondern aktiv unterbindet, bevor Schaden entsteht – unabhängig davon, ob ein Gerät im Unternehmensnetzwerk oder im Homeoffice betrieben wird.

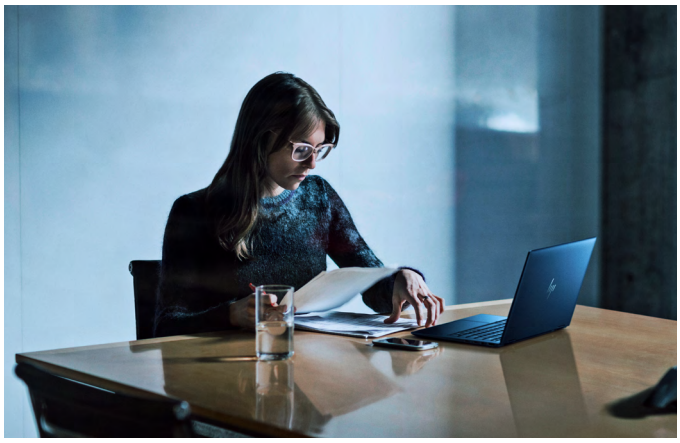
Windows Copilot+ mit integrierter NPU: Assistenz, Effizienz – und volle Governance

Assistenzfunktionen auf Basis generativer AI sind in der Arbeitswelt angekommen – doch in vielen Unternehmen ohne Kontrolle oder Integration. Genau hier setzt Windows Copilot+ an. Mithilfe einer lokal verbauten NPU mit 48 TOPS laufen Funktionen wie Click-to-Do oder Live-Untertitelung direkt auf dem Gerät – offline, datenschutzkonform und ohne Cloudabhängigkeit. Das entlastet nicht nur den First-Level-Support durch kontextbasierte Hilfestellungen, sondern beseitigt auch die Notwendigkeit externer AI-Tools. Mitarbeitende erhalten eine leistungsfähige, integrierte Assistenz – ohne auf Drittanbieter-Lösungen ausweichen zu müssen. BYOAI wird damit überflüssig. Die IT gewinnt die Hoheit über eingesetzte Tools zurück, ohne Innovationspotenziale auszubremsen.

30%

weniger First-Level-Support-Anfragen durch kontextbasierte AI-Hilfen

Quelle: HP / Microsoft Copilot+ PCs Performance Impact Report



Jetzt Wende einleiten und Governance-Power entfesseln

HP AI-Notebooks sind mehr als ein Gerätewechsel. Sie sind die Möglichkeit, eine neue Ära der IT-Strategie einzuleiten – mit klarer Rollenverteilung: Die IT steuert, automatisiert und sichert. Die Mitarbeitenden arbeiten kreativ, effizient und ohne Tool-Umwege. Die Geschäftsführung erhält Planbarkeit, Compliance-Sicherheit und reduzierte Betriebskosten. Denn wer heute in AI-PCs investiert, entscheidet nicht nur über bessere Geräte – sondern über die Rolle seiner IT-Abteilung im Unternehmen: Bleibt sie Dienstleisterin im operativen Tagesgeschäft? Oder wird sie zur Steuerzentrale für Digitalisierung, Sicherheit und Transformation?

HP AI-PCs ermöglichen diesen Wandel, weil sie nicht mehr voraussetzen, dass Innovation „nachgerüstet" wird. Governance, Automatisierung und Assistenz laufen ab Werk – strukturiert, kontrolliert, skalierbar. Damit können Entscheider Standards setzen, die in der Breite funktionieren – unabhängig von Teamgröße, Standort oder technischer Tiefe.

Doch noch wichtiger ist: Diese Investition ist kein Einzelprojekt. Sie zahlt auf zentrale Unternehmensziele ein – darunter:

- **Produktivität:** Assistenzfunktionen, die Mitarbeiter wirklich nutzen – ohne Schulungs-Overhead.
- **Talentbindung:** Moderne Work Experience, die Ansprüchen der Gen Z gerecht wird.
- **Sicherheit:** Hardwarebasierte Zero-Trust-Architekturen statt reaktive Schutzwälle.
- **Kostentransparenz:** Planbarer TCO statt ungeplante Wartung, Wildwuchs und Schattenbudgets.
- **Employer Branding:** Fortschrittliche Tools signalisieren Innovationsfähigkeit – intern wie extern.

Die drei Rollen des Entscheiders – und was HP AI-PCs jeweils ermöglichen

Rolle des Entscheiders	Herausforderung	HP AI-PC als Antwort
IT-Leiter:innen	Ressourcen, Schatten-IT, Legacy-Systeme	Struktur, Automatisierung, Sicherheit ab Werk
CFO / Geschäftsführung	Kosten, Risiko, Planbarkeit	TCO-Sicherheit, weniger Ausfall, bessere Datenbasis
CHRO / HR-Verantwortliche	Fachkräftemangel, moderne Arbeitsplätze	Attraktive Tools, Work Experience, hohe Akzeptanz

Mit AI-PCs ein starkes internes Zeichen setzen:

Wer früh auf Standards setzt, vermeidet Chaos in der Breite. Wer AI reguliert einführt, muss sie nicht unterbinden. Und wer Technologie als strategische Ressource begreift, wird Transformation nicht länger aufhalten – sondern gestalten.

Die Entscheidung für HP AI-Notebooks ist damit nicht nur richtig. Sie ist notwendig.

Informieren Sie sich noch heute, wie Sie AI in Ihren Arbeitsalltag integrieren können und Ihre Teams mit den richtigen Lösungen unterstützen können.