jamf

# **Das Playbook über neue Technologien:** Verwaltung, Schutz und Skalierung in modernen Unternehmen

## Wachstum aufstrebender Mobiltechnologien und deren Bedeutung für Unternehmen

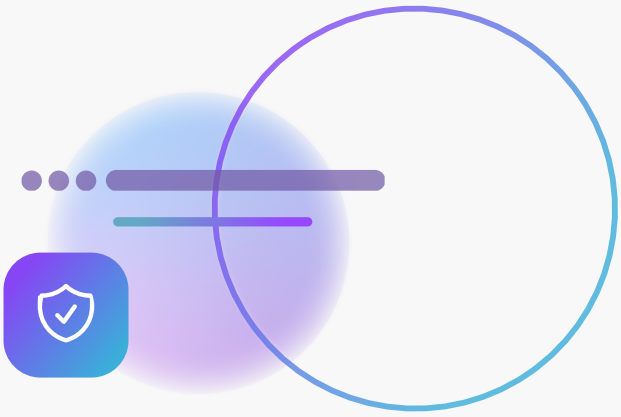
Genauso wie sich die Arbeitsumgebungen gewandelt haben, verändern neue Technologien – etwa Wearables, Spatial Computing und KI – heute die Art und Weise unserer Zusammenarbeit. Eingesetzt als Business-Tools optimieren sie das Benutzererlebnis, revolutionieren die Produktivität und treiben weltweit Innovationen in verschiedensten Branchen voran.

In diesem Zuge ist es für das Management und IT-Sicherheitsteams entscheidend, ihre Strategien für ihre Endgeräte anzupassen: Daten müssen geschützt, Geräte holistisch verwaltet und Skalierungsprozesse intelligent gestaltet werden, um Bedrohungen durch erweiterte Angriffsvektoren, lückenhafte Sichtbarkeit und den erhöhten Druck auf operative Ressourcen entgegenzuwirken.

Dieses Dokument legt nicht nur dar, warum Unternehmen ihre Verwaltung modernisieren sollten, sondern bietet auch plattformunabhängige Orientierungshilfen für den Aufbau und die Durchsetzung eines belastbaren Fundaments. Basierend auf praxisnahen Ansätzen und konkreten Handlungsschritten zeigt es auf, wie sich Komplexität reduzieren, Sichtbarkeitslücken schließen und Unternehmen auf das Zeitalter des Hybrid-Computings vorbereiten lassen.

**In diesem Dokument zeigen wir Ihnen, wie Sie:**

- Verwaltungs- und Konformitätstrategien an neue Technologien anpassen
- erkennen, warum herkömmliche Ansätze nicht die gleiche Sicherheit bieten
- Automatisierung und kontinuierliche Durchsetzung als Kernstrategien nutzen
- Management, Identität, Sicherheit und Compliance auf die Unternehmensziele abstimmen
- Zero-Trust-Sicherheit als Kernbestandteil moderner Endpunktsicherheit einsetzen



# Kurze Zusammenfassung

Unternehmen stehen am Beginn einer Ära, die von der rasanten Weiterentwicklung hybrider Computing-Modelle wie Wearables, IoT und KI definiert wird. Diese aufkommenden Technologien verändern die Geschäftsabläufe und treiben die Innovation in allen Branchen voran - aber sie bringen auch Komplexität, Fragmentierung und neue Risiken mit sich. Je vielfältiger die Geräteflotten in Unternehmen werden, desto wichtiger werden ein holistisches Management, kontextabhängige Zugriffsrichtlinien, eine fortlaufende Überprüfung des Sicherheitsstatus sowie die Einführung von Zero Trust. Deshalb sind Unternehmen, die in automatisierte Workflows, umfassende Transparenz und richtlinienbasierte Kontrollen investieren, besser aufgestellt, um Daten zu schützen, neue regulatorische Anforderungen zu erfüllen und aufstrebende Technologien mit der nötigen Sicherheit zu skalieren.

## Die wichtigsten Erkenntnisse:

- Zunahme von robusten Geräten bis 2028: **8,4 %**
- Zunahme von Spatial Computing bis 2030: **33,16 %**
- Einführung von Hybrid-Computing-Paradigmen in Unternehmen bis 2028: **40 %**
- Autonome Lösung von Service-Problemen bis 2029: **80 %**
- Verkauf von Wearables 2025: **590,7 Mio. Geräte**

# Aufstrebende Technologien – 2026 und darüber hinaus

Ein neues Zeitalter des Computings bricht an: Wearables, IoT und KI entwickeln sich von Testprogrammen zu echten Unternehmenslösungen mit messbarem Mehrwert. Sie revolutionieren, wie wir arbeiten, lernen und kommunizieren, und lassen die physische Welt immer stärker mit digitalen Workspaces verschmelzen. Das Ergebnis ist ein neues Level an Kreativität, Produktivität, Kollaboration und Automatisierung. Organisationen, die diese Dynamik nutzen, werden sich strategisch neu ausrichten, ihre Resilienz stärken, intelligent skalieren und jene Chancen ergreifen, die die nächste Stufe der Innovation definieren.

## Spatial Computing

Für viele stellte das Ende der 90er Jahre in Spielhallen verbreitete Spiel Virtual Reality (VR) Vortex den ersten Kontakt mit virtuellen Welten dar. Seither haben sich diese Technologien über Augmented Reality (AR) und Extended Reality (XR) hin zu einer Mixed Reality (MR) entwickelt, die die Brücke zwischen der physischen und der digitalen Welt schlägt.

Diese als Spatial Computing bekannte Entwicklung läutet die nächste Ära von Bildung und Produktivität ein; bis **2030 wird hier eine jährliche Wachstumsrate (CAGR) von 33,16 % prognostiziert**.

Obwohl das Spatial Computing noch in den Kinderschuhen steckt, ist der Einfluss dieser aufstrebenden Technologie bereits **weltweit in zahlreichen Branchen spürbar**, darunter im Bildungswesen, in der Fertigung und im Gesundheitswesen.

Einige Anwendungsbeispiele für den Einsatz von Spatial Computing in der Praxis:

- **Optimiertes Onboarding:** Mitarbeiter:innen lernen ihre Arbeitsplätze durch Rundgänge kennen, um neuen Kollegen bereits ab dem ersten Tag eine optimale Orientierung zu bieten.
- **Schnelles Prototyping:** Entwickler können Produkte schneller entwickeln und iterieren, während sie weiter daran arbeiten, die Stabilität zu testen und das Produkt als Team fertigzustellen.
- **Spezifische Schulungen:** Mithilfe von 3D-Overlays trainieren Chirurgen in realitätsgetreuen Szenarien. Diese immersiven Simulationen helfen dabei, komplexe Prozeduren zu erlernen und die Genauigkeit bei Operationen zu erhöhen.
- **Höhere Kundenzufriedenheit:** Einzelhandelskunden nutzen ihre Smartphones, um Produkte direkt zu Hause zu scannen und zu visualisieren oder Kleidung virtuell anzuprobieren – so werden Kunden genau dort abgeholt, wo sie sich befinden.
- **Fehlerbehebung in Echtzeit:** Die Betreiber von Maschinen nutzen Apple Vision Pro, um Probleme zu erkennen und Analysen durchzuführen, um Probleme direkt in der Produktion zu lösen.

## Wearables

Das muss man sich mal vorstellen: Eine Apple Watch enthält Hardwarekomponenten, die früher nur in Desktop-Computern der Pentium 4-Klasse möglich waren, wenn auch in miniaturisierter Form.

Dank Multi-Core-Processing, Neural Engines, einer ganzen Reihe von mikroskopisch kleinen Sensoren und der Fähigkeit, unabhängig als eigene Rechenquelle zu arbeiten, sind Arbeit (und Freizeit) heute in einem leistungsfähigen, energieeffizienten Design möglich, das direkt an Gesicht, Hand, Finger und/oder Handgelenk getragen werden kann.

Hier sind einige Anwendungsfälle für die **590,7 Millionen Wearables, die 2025 verkauft wurden**:

- **Uhr:** Vereinfachen Sie (in- und ausländische) Reisen mit GPS- und mobilfunkfähigen Smartwatches, um mit dem Büro und Ihren Angehörigen in Kontakt zu bleiben, ohne sich mit unübersichtlichen oder teuren Daten-Roaming-Tarifen herumschlagen zu müssen.
- **Tracker:** Sie erhalten aktuelle Informationen über Ihre Gesundheit, um Ihre Vitalwerte proaktiv zu überwachen, Ihre Ziele zu verfolgen oder bei Unfällen und gesundheitsbezogenen Vorfällen schnell zu reagieren und lebensrettende Hilfe zu rufen.
- **Earbuds**: Die Technologie zur Geräuschunterdrückung schränkt externe Ablenkungen ein, damit man sich besser auf das Wesentliche konzentrieren kann. Außerdem ist bei Kopplung mit einem Smartphone eine Live-Übersetzung möglich, um mehrere Sprachen in Echtzeit zu verstehen.
- **Brille**: Sie können Bilder und Videos aufnehmen, auf dringende Nachrichten antworten oder einer Wegbeschreibung folgen. Dabei haben Sie die Hände frei und der integrierte KI-Assistent hilft Ihnen, Ihr Ziel noch schneller zu erreichen.

## Internet der Dinge (IoT)

Effizienz ist ein Treiber für Geschäftskontinuität. Und da Automatisierung ein Grundbaustein für Effizienz ist, überrascht es nicht, dass Unternehmen zunehmend auf IoT-Geräte setzen, um Business Intelligence zu generieren – etwa über Prozessabläufe hinweg. Diese sind unerlässlich für jene datengesteuerten Entscheidungen, die benötigt werden, um Geschäftsabläufe umfassend zu optimieren.

Darüber hinaus werden durch die Kombination von Sensoren und Automatisierung in bestimmten Geschäftsmodellen **Energiekosteneinsparungen von ca. 20-30 %** erzielt. Und **die Wartungskosten können um bis zu 50 % gesenkt** werden, und zwar dank einer strategischen Neuausrichtung wie der vorausschauenden Wartung, die einen proaktiven Ansatz (anstelle eines reaktiven Ansatzes) bevorzugt, um ungeplante Ausfallzeiten zu reduzieren.

Einige Beispiele für die Vorteile des IoT im Unternehmen sind:

- **Asset-Tracking und logistisches Netzwerk:** Vereinfachen Sie die Bestandsüberwachung und verbessern Sie – in Kombination mit vorausschauenden Analysen – die Kapazitätsplanung sowie die Lagerprognosen.
- **Personalisierung der Customer Experience:** Stärkung der Markentreue durch maßgeschneiderte Interaktionen, die die individuellen Bedürfnisse der Kunden besser erfüllen und gleichzeitig den Service verbessern.
- **Gebäude- und Anlagenmanagement:** Reduzieren Sie Ihren Energiebedarf und steigern Sie gleichzeitig die Effizienz der Gebäudefunktionen durch Automatisieren von HLK, Beleuchtung und Sicherheit.
- **Verbindung von anspruchsvollen Systemen:** Durch die Integration von Sensoren und IoT erzielen Sie einen Mehrwert aus bestehenden Systemen und generieren neue Services und Umsatzmöglichkeiten.

## Artifizielle Intelligenz (KI)

Das Versprechen der KI betrifft Unternehmen und Privatanwender gleichermaßen. Die Vorteile von GenAI für Unternehmen scheinen grenzenlos zu sein, da die Apps weltweit in verschiedenen Industrien eingesetzt werden:

- **Höhere Wertschöpfung:** Die Mitarbeiter:innen können sich auf strategische Aufgaben konzentrieren, während repetitive Tätigkeiten automatisch ausgeführt werden.
- **ROI-Steigerung:** Die Optimierung von Ressourcen und eine höhere Effizienz verbessern Prozesse und senken die Betriebskosten – ergänzt durch qualitative Vorteile wie Innovation und ein verbessertes Kundenerlebnis.
- **Prozessoptimierung:** Maximieren Sie Ressourcen durch die schnelle Visualisierung von Konzepten, das Zusammenfassen von Inhalten oder die rasche Entwicklung von Beispielcode.
- **Optimale Analyse:** Sie gewinnen wertvolle Einblicke, führen Trendauswertungen durch und treffen proaktive, datengestützte Entscheidungen, um die Markteinführungszeiten zu verkürzen.

Darüber hinaus bietet Agentic AI (die Entscheidungen ohne menschliche Interaktion trifft) entscheidende Vorteile, die über die oben genannten Vorteile hinausgehen. So schätzt die Marktforschungsfirma Gartner, dass **bis 2029 etwa 80 % der gängigen Kundenservice-Anfragen autonom gelöst werden**. Weitere wichtige Vorteile liegen in der Fähigkeit, proaktiv (Bedrohungssuche) und adaptiv (Lernen in Echtzeit) zu sein. Ein Bereich, in dem sie entscheidende Unternehmensprozesse revolutionieren wird, ist Cybersicherheits-Software. Auf Agentic AI basierende Sicherheitslösungen überwachen und bewerten kontinuierlich Risikofaktoren und ergreifen gleichzeitig Maßnahmen zur schnellen Bedrohungsabwehr – ganz ohne menschliches Eingreifen. Dies verkürzt die Reaktionszeiten und sichert die IT-Resilienz.

## Hybrid Computing

Unternehmen weltweit stehen vor Herausforderungen in den Bereichen Effizienz, Arbeitslastbewältigung, Ressourcenbereitstellung und Skalierung. Hinzu kommen regulatorische Anforderungen und Investitionsausgaben, die herkömmliche Rechenmodelle – wie reine On-Premise-Lösungen oder öffentlichen/privaten Clouds – allein schlichtweg nicht mehr effektiv bewältigen können. Selbst Modelle mit geringerer Latenz, die Daten näher am Gerät verarbeiten, um eine schnellere Bearbeitung zu ermöglichen, wie z. B. Edge Computing, können noch nicht alle Probleme der sich schnell verändernden digitalen Landschaft lösen.

Hybrid Computing ist ein neues Paradigma, das nicht nur aufstrebende Technologien umfasst, sondern auch bestehende Computermodelle miteinander kombiniert, um diese Hindernisse zu überwinden:

- **Agilität**: Durch die Nutzung mehrerer Rechenmodelle können Unternehmen die Verkehrsabwicklung optimieren, Reaktionszeiten verkürzen und Latenzzeiten kostengünstig reduzieren, insbesondere bei unerwarteten Spitzenzeiten.
- **Leistung**: Sie erzielen Produktivitätssteigerungen durch die Implementierung KI-gesteuerter Tools und Automatisierung, um Arbeitsbelastungen intelligent auf die effizienteste Umgebung zu verteilen.
- **Konformität**: Geopatriation gibt Organisationen die Kontrolle darüber, wo Daten und Anwendungen verarbeitet und gespeichert werden. Dies sichert die Datensouveränität und erfüllt gleichzeitig Datenschutzvorgaben sowie regulatorische Anforderungen.
- **Ausfallsicherheit**: Wenn Sie die Kontinuität optimieren, können Sie dafür sorgen, dass der Geschäftsbetrieb auch bei Ausfällen aufrechterhalten wird, indem die Integration von Cloud-, On-Premises- und Legacy-Systemen genutzt wird.

Gartner prognostiziert, dass bis zum Jahr 2028 **mehr als 40 % der führenden Unternehmen Architekturen auf Basis hybrider Computing-Paradigmen** in ihre kritischen Geschäftsabläufe integriert haben werden – ein massiver Anstieg gegenüber den derzeitigen 8 %.

# Herausforderungen für die IT in den Unternehmen

Wenn Geräte außerhalb des Verwaltungsbereichs liegen, entstehen Lücken in der Sichtbarkeit, die diese Aspekte einschränken:

- Bewertung des Sicherheitsstatus
- Schnelle Reaktion auf Bedrohungen
- Aufrechterhaltung der Datensicherheit

Die Vielfalt an Plattformen und Geräten, gepaart mit unterschiedlichen Eigentumsmodellen und hybriden Arbeitsumgebungen, führt zu Variablen, die die Angriffsfläche einer Organisation vergrößern. Darüber hinaus erhöht sich der Druck auf die Teams, die bereits für die Risikominderung einer sich entwickelnden Bedrohungslandschaft verantwortlich sind. Gleichzeitig sorgen die fortschreitende Regulierung und die uneinheitlichen Standards im Bereich KI und IoT dafür, dass die Anforderungen in Bezug auf die Governance und die verantwortungsbewusste Technologieeinführung global steigen – für Unternehmen ebenso wie für deren gesamten Wirtschaftszweig

## Registrierung und Bereitstellung

Eine umfassende Verwaltungs- und Sicherheitsstrategie beginnt mit der Geräteregistrierung und bietet anschließend die Möglichkeit, Geräte mit den Tools und Konfigurationen auszustatten, die für Unternehmen notwendig sind, um die Compliance zu gewährleisten, Daten zu schützen und die Produktivität der Mitarbeiter:innen zu sichern. Diese Best Practices sind in ganzheitlichen IT-Workflows verankert und Gegenstand vieler Bereitstellungsstandards und Frameworks.

Wenn Geräte nicht in Management-Suites registriert sind oder nicht mit den Tools bereitgestellt werden, auf die ihre Benutzer zur Erledigung ihrer Aufgaben angewiesen sind, wird eine langsame, aber stetige Kette von Ereignissen in Gang gesetzt, die Risiken birgt für:

- Geräteverwendbarkeit
- Vertraulichkeit der Daten
- Integrität der Kommunikation
- Privatsphäre der Benutzer
- Verfügbarkeit der Endpunkte

Jeder Risikofaktor wirkt sich auf die Erbringung von Dienstleistungen und die Einhaltung von Vorschriften aus und hat letztlich auch Auswirkungen auf die Geschäftskontinuität.

## Richtlinien- und Transparenzlücken

Der Einblick in die Geräte ist der Eckpfeiler jeder Sicherheitsstrategie. Da der Zustand der Endgeräte weder eingesehen noch analysiert werden kann, sind IT- und Sicherheitsteams faktisch nicht in der Lage, zu erkennen, was auf den neuen Technologiegeräten geschieht. Diese Geräte verbinden sich mit der Infrastruktur, kommunizieren darüber und fordern Unternehmensressourcen an oder nutzen diese.

Aufgrund von blinden Flecken in der Telemetrie kann eine Vielzahl von Problemen auftreten, die Admins nicht lösen können, wenn sie nicht wissen, welche Bedrohungen bestehen und wie die Ressourcen angesichts begrenzter Ressourcen und/oder Entschärfungsoptionen priorisiert werden sollten.

Einige gängige Beispiele, die zu Lücken in der Sichtbarkeit führen, sind:

- Mehrere Betriebssysteme
- Physische Manipulationen
- Gemischte Besitzmodelle
- Nicht unterstützte Gerätetypen
- Fehlkonfigurationen von Geräten

## Bedrohungs- und Risikominimierung

Dass Bedrohungsakteure Hardware und Software als potenzielle Einfallstore ins Visier nehmen, ist für die Cybersicherheit nichts Neues. Die Herausforderung der Risikominimierung wird jedoch durch hybride Umgebungen erschwert: Unterschiedliche Gerätetypen, auf denen jeweils verschiedene Softwareplattformen laufen, stellen eine Vielzahl von Risiken für das Unternehmen dar.

Die Mischung aus Open-Source-, proprietären und geschlossenen Systemen und Gerätetypen belastet die IT- und Sicherheitsteams, die mit der Verwaltung und Sicherung von Endpunkten betraut sind. In Kombination mit mangelnder Sichtbarkeit des Gerätezustands und der begrenzten Fähigkeit, Geräte flächendeckend sicher zu konfigurieren, verschärfen die folgenden Herausforderungen die Schwierigkeit exponentiell, Unternehmensressourcen abzusichern:

- Sicherheit der Daten
- Ausnutzung von Schwachstellen
- Ausfallsicherheit des Netzwerks
- Patch-Verwaltung
- Größere Angriffsflächen

## Regulierungs- und Konformitätsdruck

Im Gegensatz zu vorhandenen oder alten Systemen stehen aufkommende Technologien vor einer Reihe von unterschiedlichen und sich schnell entwickelnden Herausforderungen in der globalen Landschaft. In manchen Fällen wirft das Fehlen eines einheitlichen Standards aufgrund der fragmentierten Natur der Technologien wie dem IoT viele Bedenken hinsichtlich der Datensicherheit auf. Wenn es um KI geht, herrscht weitgehend Einigkeit über die leistungsbezogenen Vorteile des Einsatzes dieser Technologie, doch weniger Menschen scheinen die Auswirkungen ihres Einsatzes auf die Menschheit oder die Umwelt zu verstehen oder sich in der Folge darüber zu einigen.

Während viele dieser Bedenken derzeit noch in Echtzeit gelöst werden, sorgen Gesetze, die sich mit der technologischen Entwicklung befassen, für eine scharfe Kontrolle. Strenge Datenschutzvorgaben wie der California Consumer Privacy Act (CCPA) und die europäische Datenschutz-Grundverordnung (DSGVO) führen dazu, dass der Einsatz neuer Technologien unter immenser Beobachtung steht. Weitere Aspekte, die von Führungskräften im Unternehmen methodisch bewertet werden müssen, um festzustellen, ob und wo sie eingesetzt werden können, sind:

- Datenresidenz
- Operative Widerstandsfähigkeit
- Risikomanagement für Drittanbieter
- Faktoren in Bezug auf die Governance
- Ethische Überlegungen

# Zukunftsweisende Lösungen und Best Practices

Bei der Bewältigung der Herausforderungen bei der Implementierung neuer Technologien sollten Unternehmen ihren Ansatz auf bewährten Best Practices basieren, um die Risikominimierung zu optimieren. Dieser disziplinierte Ansatz unterstützt eine skalierbare, widerstandsfähige Endpunktverwaltung, während die Geräteflotten immer vielfältiger werden und sich neue Anwendungsfälle entwickeln, die gezielt auf die wachsenden geschäftlichen Anforderungen zugeschnitten sind.

## Istzustand

Bevor ein Unternehmen in der Lage ist, das Risiko umfassend zu bewerten, muss es zunächst wissen, wie die Infrastruktur aussieht. Der beste Weg, sich ein Bild davon zu machen, ist eine vollständige Bestandsaufnahme aller Hardware, Software, Services und Prozesse Man braucht ein detailliertes Verständnis über:

- Jedes Gerät
- Ihre Abhängigkeiten
- Workflows und Richtlinien

Die Identifizierung jeder einzelnen Komponente und ihrer Verbindungen ermöglicht einen ganzheitlichen Überblick über die gesamte Infrastruktur, ihre Kommunikation und die beteiligten Geräte. Dies bietet Unternehmen eine solide Grundlage für die Implementierung zukunftsweisender Lösungen.

## Risikobewertung

Der nächste Schritt ist die Bewertung der Risikofaktoren, um den Schweregrad zu bestimmen. In dieser Phase geht es nicht allein darum, Risiken zu reduzieren, sondern vielmehr darum, sie mit der allgemeinen Risikobereitschaft des Unternehmens in Einklang zu bringen.

Die Kombination aus qualitativen und quantitativen Methoden ermöglicht einen programmatischen Cyber-Risiko-Index. Dieser bietet Entscheidungsträgern einen datengestützten Überblick auf Basis zentraler Angriffsindikatoren, wie zum Beispiel:

- **Vektoren**: Der Pfad oder die Methode, die zur Ausführung eines Angriffs oder zur Kompromittierung eines Systems verwendet wird.
- **Komplexität**: Die Fähigkeiten und Ressourcen, die ein Angreifer benötigt, um eine Schwachstelle auszunutzen.
- **Auswirkungen**: Die geschäftlichen und betrieblichen Folgen eines erfolgreichen Angriffs.
- **Exposition**: Die Schwachstellen oder Lücken, die ein Umfeld anfällig für Angriffe machen.
- **Schweregrad**: Ein Maß dafür, wie wahrscheinlich eine Bedrohung ist und wie viel Schaden sie potenziell anrichten kann.
- **Bekämpfung**: Ob es eine Lösung gibt, wie diese aussieht und wie schnell sie bereitgestellt werden kann.

## Modellierung von Bedrohungen

Der dritte Schritt ist ein proaktiver Ansatz zur Ermittlung und Priorisierung von Risiken auf Geräten, Systemen und Apps. Bei der Modellierung von Bedrohungen vor Penetrationstests (mehr dazu im nächsten Abschnitt) liegt der Schwerpunkt auf der Priorisierung der Risiken vom höchsten zum niedrigsten Schweregrad. Dies wiederum trägt nicht nur zur Verringerung des Geräterisikos bei, sondern auch zur Aufrechterhaltung des Sicherheitsstatus im Unternehmen.

Es gibt mehrere Bedrohungsmodelle, die zur Bewertung spezifischer Risikotypen oder als integrierter Ansatz zur systematischen Ermittlung und Quantifizierung von Bedrohungen verwendet werden können. Das bedeutet: Der beste Weg, um einen Angreifer zu bekämpfen, ist, wie einer zu denken.

**Gängige Methoden zur Modellierung von Bedrohungen und ihre Anwendung sind:**

STRIDE:
Spoofing, Manipulation, Zurückweisung, Offenlegung von Informationen, Dienstverweigerung und Erweiterung von Berechtigungen.
WAS ES TUT:
Dieses Modell kategorisiert das Risiko auf der Grundlage seiner Leistung in jeder der sechs Kategorien.

DREAD:
Schadenspotenzial, Reproduzierbarkeit, Ausnutzbarkeit, betroffene Benutzer*innen und Entdeckbarkeit.
WAS ES TUT:
Mit diesem Modell wird auf der Grundlage der fünf Faktoren ein Durchschnittswert ermittelt, um den Schweregrad des Risikos einzustufen. (Es wird oft in Verbindung mit STRIDE verwendet, um Bedrohungen mit hohem Risiko vorrangig zu bekämpfen).

LINDDUN:
Verlinkung, Identifizierung, Nichtabstreitbarkeit, Erkennung, Offenlegung von Daten, Unkenntnis und Non-Compliance.
WAS ES TUT:
Dieses Modell bietet eine strukturierte Methode zur Ermittlung und Eindämmung von datenschutzrelevanten Bedrohungen, die auf der Analyse des Datenflusses innerhalb von Apps und Systemen beruht.

PASTA:
Verfahren zur Simulation von Angriffen und zur Analyse von Bedrohungen.
WAS ES TUT:
Dieses Modell konzentriert sich auf die Auswirkungen von Risiken auf Unternehmen, einschließlich technischer Anforderungen (z. B. Definition von Zielen und Umfang, Analyse von Schwachstellen und Simulation von Angriffen), für die Entwicklung von Strategien zur Risikominderung.

OCTAVE:
Bewertung von Bedrohungen, Assets und Schwachstellen im Zusammenhang mit dem Betrieb.
WAS ES TUT: Dieses Modell konzentriert sich auch auf Geschäftsrisiken, die die Cybersicherheit mit den Unternehmenszielen in drei Phasen in Einklang bringen: Erstellung von anlagenbasierten Bedrohungsprofilen, Identifizierung von Schwachstellen in der Infrastruktur und Entwicklung von Risikomanagementstrategien.

## Penetrationstests

Die wohl häufigste Aufgabe bei der Bewertung von Risiken ist der Penetrationstest, der häufig durchgeführt wird, um Schwachstellen in Geräten und Software zu finden und zu beseitigen. Die Entscheidung, dies als letzten Punkt in die Liste aufzunehmen, geht auf den vorherigen Abschnitt über die Modellierung von Bedrohungen zurück. Wird der Penetrationstest nach der Bedrohungsmodellierung durchgeführt, erhöht er die Effizienz und Effektivität des Risikobewertungsprozesses.

Dies wird durch folgende Aspekte erreicht:

- Penetrationstests können sich auf Risiken mit höherem Schweregrad konzentrieren (da die Bedrohungsmodellierung wahrscheinlich bereits Bedrohungen mit geringerem Risiko identifiziert)
- Einfachere Risikominimierung durch IT in einem früheren Stadium des Bewertungsprozesses

Für letztere:

- Der Test validiert zuvor bereitgestellte Vorschläge zur Problemlösung
- Die Suche nach Schwachstellen, die zuvor möglicherweise unbemerkt geblieben sind, wird um eine weitere Prüfungsebene ergänzt

## Gerätezustand und identitätsbasierter Zugang (Zero-Trust Journey)

Neue Technologien erfordern Identitätsstrategien und eine kontinuierliche Validierung des Gerätezustands, um sensible Daten zu schützen und die betriebliche Integrität aufrechtzuerhalten. Die Modernisierung des Managements zur Unterstützung zunehmend diversifizierter Flotten muss die Durchsetzung automatisieren, den betrieblichen Aufwand reduzieren und Zero-Trust nahtlos skalieren.

Die folgenden Lösungen bieten variable Tools zur Unterstützung der IT beim Lebenszyklus-Management neuer Technologien:

- **Mobile Device Management (MDM)**: integriert die Geräte- und Identitätsverwaltung sowie die Endpunktsicherheit umfassend - **von der Zero-Touch-Bereitstellung bis zur sicheren Entsorgung** - vor Ort oder Cloud-basiert.
- **Unified Endpoint Management (UEM)**: vor Ort oder in der Cloud, bietet plattformübergreifenden Support, allerdings oft im Austausch für einen eingeschränkteren Funktionsumfang.
- **Amazon Web Services (AWS):** Cloud-basiertes Modell, das Verwaltbarkeit und Sicherheit bietet, die auf bestimmte Technologien, wie IoT-Geräte, beschränkt sind und mehrere Anbieter unterstützen.
- **Autonomous Endpoint Management (AEM):** die Zukunft des Cloud-basierten UEM, das die Betriebskosten durch mehr Automatisierung senkt und Zero-Trust durch kontinuierliche Validierung und Korrektur des Gerätezustands durchsetzt – für diversifizierte Flotten und in großem Umfang.

## App- und Datenkontrolle

Im Wesentlichen sind Daten - unabhängig vom Gerätetyp oder vom OS, mit dem sie ausgeführt werden - Daten. Der Schutz von Daten bildet weiterhin den Kern jeder Kontrolle, jedes Prozesses und jeder Aufgabe, die im Rahmen der Verwaltung und Absicherung neuer Technologien durchgeführt werden.

Das Bereitstellen von Konfigurationen ist eine wirksame Methode, um Geräte und die auf ihnen verarbeiteten und enthaltenen Daten zu schützen. Obwohl die unterstützten Methoden weitgehend von der jeweiligen Betriebssystem-Plattform abhängen, ist es das Ziel, sichere Konfigurationen auf Basis von Best Practices zu etablieren. Hierzu zählen Standards und Frameworks, die über Betriebssystemgrenzen hinweg anwendbar sind, um die Datensicherheit zu gewährleisten.

Beispiele für Tools, die zur Erstellung sicherer Konfigurationen verwendet werden, sind:

- **Android**: **OEMConfig** und **Android Open Source Project** (AOSP)
- **Apple**: **Apple Configurator**, **Jamf Pro** und **Deklarative Geräteverwaltung** (DDM)
- **Linux**: Bash-Skripte, **SOTI MobiControl** und **Microsoft Intune**
- **Proprietäre Tools:** Auf der Support-Website des Herstellers finden Sie Informationen darüber, wo Sie spezifische Tools erhalten.

## Überwachung und Reaktion

Die Transparenz über den Zustand der Endpunkte ist ein wesentlicher Bestandteil der proaktiven Cybersicherheit. Je früher Probleme erkannt werden, desto schneller kann die Reaktion auf Vorfälle das Risiko minimieren oder die Bedrohung abwehren. Die aktive Überwachung der Endpunkte innerhalb Ihrer Infrastruktur ist nicht nur äußerst empfehlenswert, sondern auch eine entscheidende Komponente einer Zero-Trust-Architektur.

Schutzmechanismen auf dem Endgerät und innerhalb des Netzwerks bilden die beiden Säulen der Zero-Trust-Sicherheit. Hier finden Sie Richtlinien, die sich auf die Endpunkte konzentrieren, um einen sicheren Gerätezustand in Ihrer Infrastruktur zu gewährleisten:

- Aktive Überwachung der Telemetrie zum Gerätezustand und der Konformitätsstufen
- Integration von Verwaltungs- und Sicherheitslösungen zur Automatisierung von Reaktionen auf Vorfälle
- Implementierung von Zero-Trust, um den Zustand der Endpunkte zu überprüfen, bevor sie Zugang auf Ressourcen erhalten
- Regelmäßige Bereitstellung von Updates für Betriebssysteme sowie Sicherheits- und App-Patches

## Netzwerksicherheit

Neue Technologien überholen oft die Standards, was die Verwaltung bestimmter Endpunkte erschwert oder zu einer Diskrepanz zwischen Technologie und Geschäftszielen führt. Da Risiko subjektiv ist, gibt es keine universellen Sicherheitsstrategien. Dadurch rückt der Schutz von Daten auf den Endpunkten in den Vordergrund. Die folgenden Lösungen - ob einzeln bereitgestellt oder kombiniert - tragen zur Maximierung der Datensicherheit in lokalen und Cloud-Umgebungen bei:

- **Demilitarisierte Zonen (DMZ)**: segmentiert Geräte mit hohem Risiko, wie z. B. IoT, und lässt nur kontrollierte Kommunikation mit internen Systemen oder externen Netzwerken auf der Grundlage von Richtlinien zu.
- **Virtuelles lokales Netzwerk (VLAN)**: isoliert den Netzwerkverkehr – wodurch die Seitwärtsbewegung begrenzt und die Kommunikation nach dem Least-Access-Prinzip erzwungen wird – und bietet der IT eine granulare Kontrolle über den Datenverkehr zwischen Geräten und geschäftskritischen Systemen.
- **Sicherheitsorchestrierung, Automatisierung und Reaktion (SOAR)**: vereinheitlicht Sicherheitstools und Workflows durch Automatisierung, um die Erkennung, Reaktion und Eindämmung von Bedrohungen zu beschleunigen.
- **Zero-Trust-Netzwerkzugriff (ZTNA)**: kontinuierliche, kontextbasierte Geräteüberprüfung, Microtunneling (pro Verbindungsanfrage) und Zustandschecks, um sicherzustellen, dass nur konforme Geräte Zugang zu geschützten Ressourcen haben.

## Baselines und Benchmarks, Standards und Frameworks

Es ist wichtig, jeden Abschnitt als eine zyklische Phase und nicht als eine lineare Phase zu betrachten. IT- und Sicherheitszyklen sind iterative Prozesse. Sie sind kein Endzustand, sondern ein kontinuierlicher Prozess, bei dem künftige Schritte auf den Erkenntnissen der Vergangenheit aufbauen und durch diese maßgeblich bestimmt werden. In diesem Sinne ist die Synergie zwischen den folgenden Aspekten von entscheidender Bedeutung, um die Sicherheit aufrechtzuerhalten und gleichzeitig neue Technologien in Ihr technisches System zu integrieren:

- **Baselines:** eine Sammlung von Kontrollen und Verfahren, die **einen grundlegenden Sicherheitsstatus definieren.**
- **Benchmarks:** Leistungskennzahlen zur **Messung der Konformität mit bewährten Sicherheitspraktiken.**
- **Standards:** weltweit anerkannte Best Practices, die angeben, wie sichere Hardware, Software und/oder Services **geschützt werden sollten, um eine bestimmte Anforderung zu erfüllen**.
- **Frameworks:** strukturierte Richtlinien, die detailliert beschreiben, wie Kontrollen, Richtlinien, Prozesse und **Standards bereitgestellt werden sollten, um Risiken zu minimieren** und die Sicherheit zu maximieren.

## Fazit

Mit dem Verständnis für neue Technologien und deren Auswirkungen auf die Unternehmensziele ist jetzt für Führungsebene und IT-Teams der Moment gekommen, den nächsten Schritt zu gehen: bestehende Management- und Sicherheitsstrategien mit zukunftsorientierten Best Practices in Einklang zu bringen. Wenn Organisationen jetzt handeln, können sie aufkommenden Risiken einen Schritt voraus sein, ihre Abläufe optimieren und selbstbewusst in die nächste Ära der Innovation eintreten.

## Checkliste: Nächste Schritte für Business Manager und IT-Manager

### 1. Identifizierung von Geschäftsanwendungsfällen

- Bewerten Sie, wo aufkommende Technologien (AI, IoT, Spatial Computing, Wearables) mit den Unternehmenszielen übereinstimmen.
- Ermitteln Sie den potenziellen ROI und betriebliche Verbesserungen im Vergleich zu bestehenden Workflows.
- Setzen Sie vorrangig Initiativen um, die messbare Geschäftsergebnisse liefern und die dazu beitragen, die Vorschriften einzuhalten.

### 2. Etablierung eines funktionsübergreifenden Bewertungsteams

- Bilden Sie ein Gremium mit Stakeholdern aus den Bereichen IT, Sicherheit, Recht und Betrieb.
- Ernennen Sie Verantwortlich für Risikobewertung, Compliance-Überprüfung und Lebenszyklus-Management.
- Definieren Sie Kommunikationskanäle für schnelles Feedback und Eskalation.

### 3. Durchführung einer umfassenden Bestandsaufnahme der Assets und Abhängigkeiten

- Erfassen Sie alle Geräte, Software, APIs und Cloud Services, die innerhalb der Infrastruktur verwendet werden.
- Identifizieren Sie die jeweiligen Abhängigkeiten bei der Integration in hybride Umgebungen (Cloud, On-Premise und Edge).
- Markieren Sie die Geräte nach dem jeweiligen Besitzverhältnis (COBO/COPE/BYOD/CYOD), um Sichtbarkeit und Verantwortlichkeit zu gewährleisten.

### 4. Bewertung von Risiken und Bedrohungen

- Nutzen Sie sowohl qualitative als auch quantitative Methoden, um die Risikotoleranz und die Auswirkungen abzuschätzen.
- Nutzen Sie Modelle für das Threat Mapping, um präzise und konsistente Ergebnisse zu erzielen.
- Stufen Sie Ihre Schwachstellen nach Schweregrad, Ausnutzbarkeit und Zeitrahmen für die Behebung ein.

### 5. Durchführung einer Bedrohungsmodellierung

- Simulieren Sie potenzielle Angriffswege mithilfe anerkannter Frameworks zur Modellierung von Bedrohungen.
- Identifizieren Sie Risikopunkte in den Bereichen Datenschutz, Datenfluss und Betrieb.
- Dokumentieren Sie Maßnahmen zur Risikominimierung vor dem Rollout.

### 6. Validierung der Anforderungen in Bezug auf Compliance und Governance

- Schauen Sie sich regionale und branchenspezifische Vorschriften an.
- Überprüfen Sie die Datenresidenz, die Souveränität und das Risikomanagement von Drittanbietern.
- Integrieren Sie ethische Überlegungen in den Einsatz von KI und datenbasierten Technologien.

### 7. Definition der Prozesse zur Registrierung und Bereitstellung

- Standardisieren Sie Ihre Onboarding-Workflows für alle Gerätetypen und Besitzmodelle.
- Automatisieren Sie Konfiguration, Patching-Kadenz und Zugangskontrollen, um manuelle Fehler zu minimieren.
- Verwenden Sie eine sichere Registrierung und identitätsbasierte Authentifizierung, um die Endpunkte zu verifizieren.

## 8. Integration identitätsbasierter Zugangsstrategien

- Verlangen Sie eine kontinuierliche Verifizierung von Anmeldedaten und Gerätestatus vor jedem Ressourcenzugriff.
- Nutzen Sie das Prinzip der geringsten Berechtigungen für Ihre Endgeräte und Apps.
- Integrieren Sie Zero-Trust und kontextbasierte Richtlinien in die Zugangskontrollsysteme.

## 9. Etablierung einer sicheren Konfigurations- und Datenkontrolle

- Definieren Sie Sicherheits-Baselines, um die Erwartungen in Bezug auf Konfiguration und Compliance festzulegen.
- Verschlüsseln Sie sensible Daten im Ruhezustand und bei der Übertragung.
- Implementieren Sie detaillierte Richtlinien für die Klassifizierung, Speicherung und gemeinsame Nutzung von Daten.

## 10. Segmentierung und Sicherung der Netzwerkkommunikation

- Verwenden Sie VLANs und DMZs, um Geräte mit hohem Risiko, wie IoT und Wearables, zu isolieren.
- Nutzen Sie Mikrosegmentierung und Zero-Trust-Netzwerkzugriff (ZTNA) für anpassbare, netzwerkinterne Sicherheitskontrollen.
- Datensicherheit muss das Herzstück der Netzwerksicherheit bilden. Dies gilt unabhängig davon, welche Geräte genutzt werden, wem diese gehören, welches Betriebssystem installiert ist oder von wo aus die Mitarbeiter:innen arbeiten.

## 11. Implementierung von Richtlinien zur kontinuierlichen Überwachung und automatisierten Reaktion

- Sammeln Sie Telemetriedaten von allen Endpunkten, um Transparenz und Erkenntnisse in Echtzeit über den Zustand zu erhalten.
- Implementieren Sie automatisierte Workflows für die Erkennung von Anomalien und die Reaktion auf Vorfälle.
- Streamen Sie Warnmeldungen in zentralisierte Tools, um Aufgaben zur Erkennung und Behebung von Bedrohungen zu automatisieren.

## 12. Verwendung von Baselines, Benchmarks und Sammlung von Produktivitätskennzahlen

- Setzen Sie grundlegende Sicherheitsstandards für eine ganzheitliche Konfiguration im Unternehmen ein.
- Verwenden Sie Benchmarks zur Messung der Leistung und des Sicherheitsstatus.
- Überprüfen Sie die KPIs zur Bewertung des Compliance-Status und zum Nachweis der Risikominimierung.

## 13. Regelmäßige Validierungen: Penetrationstests und Audits

- Planen Sie wiederkehrende Penetrationstests und Schwachstellen-Scans nach der Implementierung ein.
- Validieren Sie die Lösungsvorschläge, die sich bei der Bedrohungsmodellierung ergeben haben.
- Überprüfen Sie die Ergebnisse anhand festgelegter Baselines und aktualisieren Sie die Richtlinien bei Bedarf.

## 14. Automatisierung des Lebenszyklus-Managements und Durchsetzung von Richtlinien

- Nutzen Sie Unified Endpoint Management (UEM) oder autonome Systeme für die laufende Compliance.
- Automatisieren Sie Prozesse für Patches, Richtlinien für die Konformität und Workflows zur Außerbetriebnahme von Geräten.
- Passen Sie Ihre Konfigurationen kontinuierlich an sich entwickelnde Frameworks und Standards an.

## 15. Dokumentation der Ergebnisse und regelmäßige Durchführung von Schulungen

- Implementieren Sie Feedback-Schleifen für neue Bedrohungen und Lessons Learned.
- Bieten Sie kontinuierlich Schulungen für Admins und Benutzer zur Erkennung von Risiken an.
- Überprüfen Sie die Eignung und passen Sie die Kontrollen an, wenn sich die Technologien und Vorschriften ändern.