Copilot-Kontrollsystem
Deep Dive Handbuch

Anleitung zur effektiven Überwachung und Verwaltung von Copilot

⚠️ Hinweis

Achtung! Dieses Dokument wurde auf Basis der Transkripte der zehn Sessions des *Copilot Control System Deep Dive* Events mithilfe des Research Agenten von Microsoft 365 Copilot erstellt. Es wurden **keine** Faktchecks, Richtigstellungen oder redaktionellen Überarbeitungen vorgenommen.

Dieses Dokument stellt lediglich ein **Proof of Concept** dar, wie man aus Videoinhalten ein thematisch fokussiertes Handbuch für eine bestimmte Zielgruppe und einen konkreten Anwendungszweck generieren kann.

Die Nutzung erfolgt auf eigene Gefahr.

Einleitung

Das Copilot-Kontrollsystem ist ein Rahmenwerk aus Sicherheits-, Verwaltungs- und Messpraktiken, das sicherstellt, dass Microsoft 365 Copilot und seine KI-gesteuerten Agenten in einem Unternehmen effektiv und sicher eingesetzt werden. Dieses Handbuch fasst die Erkenntnisse aus einer zehnsitzigen Deep-Dive-Veranstaltung in praktischer Anleitung für Entscheidungsträger zusammen – die Führungskräfte, die für die Implementierung von Copilot, die Überwachung seiner Nutzung und die Realisierung seines Werts verantwortlich sind.

Jeder Abschnitt entspricht einer der Sitzungen der Veranstaltung und erläutert deren Bedeutung, häufige Herausforderungen sowie empfohlene Werkzeuge und Methoden zur Überwachung und Verwaltung von Copilot. Der Ton ist zugänglich und handlungsorientiert und konzentriert sich auf das „Was“ und „Wie“ in praxisnahen Begriffen, anstatt auf technische Details einzugehen.

Inhaltsverzeichnis

Jeder Abschnitt kann für sich allein stehen, um einen bestimmten Verwaltungsbereich zu behandeln. Zusammen bilden sie einen umfassenden Leitfaden für die Einführung von Copilot in einem Unternehmen auf kontrollierte und messbare Weise. Entscheidungsträger können dies als Fahrplan nutzen, um Innovation mit Governance in Einklang zu bringen – und so die Vorteile von Copilot zu maximieren, während Sicherheit, Compliance und Benutzerzufriedenheit gewahrt bleiben.

Quellenhinweise

Basierend auf den Copilot Control System Deep Dive Sessions

- https://techcommunity.microsoft.com/event/microsoft365copilot-events/digital-deep-dive-copilot-control-system-ccs/4414752
- https://adoption.microsoft.com/de-de/copilot/control-system/

Erstellt von Michael Greth (MVP) yourcopilot.de - mit dem Research Agent in Microsoft 365 Copilot (22. Juni 2025)
Übersetzt mit Gemini 2.5

1. Überblick über das Copilot-Kontrollsystem – Governance-Säulen und ihre Bedeutung

Schlüsselthemen: Die Veranstaltung begann mit der Vorstellung der drei Kernsäulen des Copilot-Kontrollsystems:

- **Sicherheit & Governance,**
- **Verwaltungskontrollen,** und
- **Messung & Berichterstattung.**

Diese Säulen bieten einen strukturierten Ansatz für die Implementierung von Copilot in einem Unternehmen. Entscheidungsträger lernten die Gesamtstrategie für den Einsatz von KI-Assistenten (Copilot und benutzerdefinierte „Agenten“) im großen Maßstab kennen und wie diese Säulen miteinander verbunden sind, um den Erfolg sicherzustellen.

Warum es wichtig ist: Dieser Überblick schuf die Grundlage für alle nachfolgenden Sitzungen. Für Entscheidungsträger ist es entscheidend, das große Ganze zu verstehen. Die Einführung von Copilot ist nicht nur ein IT-Projekt – es ist eine Veränderung der Arbeitsweise der Mitarbeiter. Die drei Säulen stellen sicher:

- **Sicherheit & Governance:** Die Nutzung von Copilot bleibt konform mit Datenschutz- und Sicherheitsrichtlinien.
- **Verwaltungskontrollen:** Administratoren können Copilot und KI-Agenten konfigurieren, überwachen und verwalten, um eine unkontrollierte Ausbreitung oder Missbrauch zu verhindern.
- **Messung & Berichterstattung:** Organisationen können die Akzeptanz, Produktivitätssteigerungen und den Return on Investment (ROI) verfolgen.

Ein ganzheitliches Kontrollsystem schafft **Vertrauen** – Mitarbeiter vertrauen dem Werkzeug (da sie wissen, dass es ordnungsgemäß gesteuert wird), und die Führungsebene vertraut darauf, dass Risiken gemanagt und Vorteile messbar sind. Ohne diese Grundlage könnten spätere technische Lösungen oder Akzeptanzbemühungen aufgrund unkontrollierter Risiken oder unklaren Nutzens scheitern.

Herausforderungen: In dieser Phase besteht die primäre Herausforderung oft darin, organisatorische Zustimmung und eine klare Vision zu erhalten. Entscheidungsträger müssen Silos zwischen IT, Sicherheit und Geschäftsbereichen aufbrechen:

- Sicherstellen, dass **Sicherheits- und Compliance-Beauftragte** darauf vertrauen, dass Copilot Standards erfüllt (z.B. keine Lecks sensibler Daten).
- **IT-Managern** versichern, dass sie die notwendigen Kontrollen haben werden, um Benutzer zu unterstützen und die Nutzung zu skalieren.
- **Führungskräfte aus den Geschäftsbereichen** davon überzeugen, dass Copilot die Produktivität steigern kann und die Investition wert ist, was klare Metriken erfordert.

Zusätzlich kann in Organisationen Unklarheit darüber bestehen, wer die Copilot-Governance verantworten sollte – es ist eine multidisziplinäre Anstrengung.

Werkzeuge & Methoden: Um diese Herausforderungen anzugehen und eine starke Grundlage zu schaffen, werden die folgenden Werkzeuge und Methoden verwendet:

- **Copilot Control System Framework:** Ein dokumentierter Plan, der Sicherheits-, Verwaltungs- und Messaufgaben aufeinander abstimmt.
- **Rollen- & Verantwortlichkeitsmatrix:** Eine Tabelle, die klärt, wer (IT, Sicherheit, Business, HR) für jede Säule verantwortlich ist (siehe Tabelle 1 unten).
- **Initiale Risikobewertung:** Ein Workshop oder Audit zur Identifizierung potenzieller Compliance- oder Sicherheitsrisiken bei der Einführung von Copilot (z.B. Datenkategorien, auf die Copilot zugreifen könnte, regulatorische Anforderungen).
- **Governance-Komitee:** Bildung eines funktionsübergreifenden Teams (Entscheidungsträger aus IT, Sicherheit, Daten und Geschäftsbereichen), um die Einführung zu steuern. Dieses Komitee trifft sich regelmäßig (z.B. alle zwei Wochen), um Fortschritte und Probleme zu überprüfen.
- **Kommunikationsplan:** Frühzeitige Kommunikation an Mitarbeiter und Stakeholder über die Einführung von Copilot, die erklärt, „was es ist“, „warum wir das tun“ und „wie es gesteuert wird“. Dies hilft, Erwartungen zu setzen und Unsicherheit zu reduzieren.

Tabelle 1. Beispielhafte Rollen & Verantwortlichkeiten für die Copilot-Governance

Rolle	Hauptverantwortlichkeiten	Beteiligung an Säulen
IT-Administrator	Copilot-Einstellungen konfigurieren; Verfügbarkeit aufrechterhalten; Leistung überwachen.	Verwaltungskontrollen; Berichterstattung (technische Metriken).

Sicherheits-/Compliance-Leitung	Zugriffsrichtlinien festlegen; Datenverbindungen genehmigen; DLP und Compliance durchsetzen.	Sicherheit & Governance; Verwaltungskontrollen (Richtlinien).
Business-Sponsor (z.B. COO)	Erfolgskriterien definieren; sicherstellen, dass Copilot mit den Geschäftszielen (Produktivität) übereinstimmt.	Messung & Berichterstattung; Akzeptanzstrategie.
Datenschutzbeauftragter	Datenschutzimplikationen überwachen; Einhaltung von DSGVO oder anderen Vorschriften sicherstellen.	Sicherheit & Governance.
Akzeptanz- & Schulungsleitung (z.B. HR oder Change Manager)	Schulungsprogramme entwickeln; Best Practices fördern; Benutzerengagement vorantreiben.	Verwaltungskontrollen (Maker-Befähigung); Messung (Benutzerfeedback).

Mit diesen Governance-Strukturen ist die Organisation bereit, sich mit den Details zu befassen – von den Kontrollen der Websuche bis zur Benutzerschulung – mit einem gemeinsamen Verständnis der Ziele und Leitplanken. Die folgenden Abschnitte gehen auf jedes Hauptthema ein und bieten Entscheidungsträgern eine Anleitung zur praktischen Umsetzung und Überwachung für jeden Bereich.

2. Websuche-Integration und -Kontrolle – Antworten mit aktuellen Daten (und Leitplanken) verbessern

Eine der ersten Deep-Dive-Sitzungen konzentrierte sich auf die **Websuche-Integration** von Microsoft 365 Copilot. Copilot kann seine Antworten erweitern, indem er Echtzeit-Websuchen durchführt – er zieht die neuesten Daten aus dem Internet, um Benutzeranfragen zu beantworten (zum Beispiel aktuelle Nachrichten oder Live-Marktpreise, die über die internen Dokumente des Benutzers hinausgehen). Diese Funktion macht die Antworten von Copilot **aktueller und umfassender**. Sie wirft jedoch auch Fragen zur Governance auf: Wie stellen wir sicher, dass die Webergebnisse angemessen, sicher und konform sind?

Bedeutung für Entscheidungsträger:

Für Entscheidungsträger geht es bei der Kontrolle der Websuche darum, ein Gleichgewicht zwischen **Antwortqualität und Risikomanagement** zu finden. Frische, relevante Daten aus dem Web können die Nützlichkeit von Copilot erheblich verbessern (z. B. die Recherche nach den neuesten Produkten eines Anbieters oder Reisehinweisen, wie in den Demonstrationen der Veranstaltung gezeigt). Dies kann den Mitarbeitern Zeit sparen, da manuelle Websuchen entfallen. Aber Führungskräfte müssen sicherstellen, dass:

- **Produktivitätsgewinne** nicht auf Kosten von **Compliance-Verstößen** gehen (z. B. durch versehentliches Anzeigen unangemessener Inhalte).
- **Webergebnisse** den Inhaltsstandards und Sicherheitsfilterungen der Organisation entsprechen (keine Malware, Desinformation usw.).
- Das **Benutzervertrauen** gewahrt bleibt, indem transparent gemacht wird, wann Copilot Webdaten verwendet und welche Quellen er nutzt.

Herausforderungen:

Zu den wichtigsten diskutierten Herausforderungen und Bedenken gehörten:

- **Datenschutz:** Könnte Copilot beim Senden einer Anfrage an Bing interne Prompts oder Daten preisgeben? (Zum Beispiel ein Prompt, der einen Kundennamen oder einen Projektcode enthält – Führungskräfte befürchten, dass diese Anfrage extern protokolliert werden könnte.)
- **Ungenauer oder ungeeigneter Inhalt:** Das Live-Web kann ungeprüfte Informationen enthalten. Ohne Kontrollen könnte Copilot Antworten aus minderwertigen oder nicht konformen Quellen zurückgeben.

Entscheidungsträger befürchten Fehlinformationen oder sogar das Auftauchen anstößiger Inhalte.

- **Umgehung von Richtlinien durch Benutzer:** Wenn die Websuche aktiviert ist, könnten Benutzer absichtlich oder versehentlich Daten abrufen, die sie nicht abrufen sollten (zum Beispiel unter Umgehung unternehmenseigener Rechercheverfahren).
- **Administrativer Aufwand:** Wie können die bestehenden Webfilter oder Safe-Search-Einstellungen des Unternehmens effektiv auf den Webzugriff von Copilot angewendet werden, ohne ein komplett neues System zu benötigen?

Werkzeuge & Methoden zur Überwachung und Verwaltung:

Microsoft bietet mehrere Kontrollebenen, um sicherzustellen, dass die Nutzung der Websuche durch Copilot sicher und überschaubar ist. Die Sitzung skizzierte einen „Vier-Ebenen-Schutz"-Ansatz, der in Tabelle 2 zusammengefasst ist:

Tabelle 2. Vier Ebenen des Websuche-Schutzes in Copilot

Schutzebene	Beschreibung & Zweck	Admin-Kontrollen	Benutzererfahrung
1. Admin-Kontrollen	Organisationsweite Richtlinien, die steuern, ob und wie Copilot die Websuche nutzen kann. Gewährleistet die Übereinstimmung mit der Unternehmensrichtlinie.	Websuche für Gruppen oder den gesamten Tenant aktivieren/deaktivieren; einschränken, welche Benutzer den Web-Modus vs. Arbeits-Modus nutzen können.	Websuche-Schalter nur sichtbar, wenn erlaubt; Benutzer sehen eine gebrandete Erfahrung (z. B. „Bing"-Ergebnisse).
2. Benutzerschutz	In-Produkt-Kontrollen für Benutzer: klare Indikatoren für Webinhalte und die Möglichkeit, die Websuche für persönliche Anfragen zu deaktivieren.	N/A (Einstellung auf Benutzerebene)	„Web:"-Präfix bei Zitaten; Benutzer-Schalter im Copilot-Chat („Webergebnisse einbeziehen"-Schalter).

3. Anfrage-Schutzmaßnahmen	Automatisierte Filter für die Anfragen, die Copilot an Bing sendet: entfernt Unternehmensidentifikatoren, blockiert sensible Begriffe oder lange Daten. Verhindert unbeabsichtigte Datenexposition in Webanfragen.	Konfigurierbar über Data Loss Prevention (DLP)-Richtlinien (behandelt ausgehende Anfragen wie Daten, die geschützt werden müssen).	Wenn eine Anfrage blockiert wird, informiert Copilot den Benutzer („Ich kann dafür nicht im Web suchen“).
4. Vertragliche Verpflichtungen	Microsofts Garantien und technische Maßnahmen: Webanfragen werden nicht zum Erstellen von Werbeprofilen verwendet und entsprechen den Datenschutzstandards. Bietet die Gewissheit, dass die Nutzung von Bing über Copilot die Daten-Governance nicht beeinträchtigt.	Definiert in den Produktbedingungen (keine Admin-Aktion erforderlich; Transparenzberichte verfügbar).	Größtenteils unsichtbar für den Benutzer; Backend-Prozess stellt sicher, dass Unternehmensanfragen isoliert und nicht über den Geltungsbereich hinaus aufbewahrt werden.

Praktische Methoden zur Überwachung und Verwaltung der Websuche-Nutzung umfassen:

- **Audit-Protokolle & Warnungen:** Das Copilot-Kontrollsystem kann Webanfrage-Ereignisse protokollieren. Administratoren können Warnungen für ungewöhnliche Spitzen einrichten (z. B. wenn ein Konto plötzlich 100 Webanfragen in einer Stunde stellt, was auf möglichen Missbrauch hindeutet).
- **Communication Compliance (in Microsoft Purview):** Dieses Tool kann die Websuchanfragen von Copilot auf sensible Informationen scannen (z. B. wenn jemand einen Prompt-Injection-Angriff versucht oder vertrauliche Begriffe in eine Webanfrage eingibt). Es kennzeichnet riskantes Verhalten zur Überprüfung durch den Administrator, ohne die legitime Nutzung zu blockieren.

- **Regelmäßige Richtlinienüberprüfungen:** Entscheidungsträger sollten regelmäßig überprüfen, ob das von Bing bereitgestellte Standard-Sicherheitsniveau ausreicht und ob internes Feedback nahelegt, dass bestimmte Domains blockiert oder zugelassen werden sollten. Dies ähnelt der Aufrechterhaltung einer sicheren Browser-Richtlinie für Mitarbeiter – der Unterschied ist, dass Copilot das Surfen übernimmt.
- **Benutzeranleitung & Schulung:** Ein praktisches Handbuch für Benutzer (anders als dieses Handbuch für Entscheidungsträger) kann Mitarbeiter anleiten, wie sie webfähigen Copilot effektiv nutzen. Zum Beispiel: „Verwenden Sie den Web-Modus für allgemeine Wissensfragen. Vermeiden Sie die Eingabe von Kundengeheimnissen, wenn das Web aktiviert ist.“ Diese Richtlinien verbessern sowohl die Ergebnisse als auch die Risikominderung.

Durch den Einsatz dieser Ebenen und Methoden können Entscheidungsträger die Websuche von Copilot **sicher per Design** aktivieren. Das bedeutet, dass Mitarbeiter von Echtzeit-Antworten profitieren, jedoch innerhalb von Grenzen: Admin-Richtlinien beschränken die breite Nutzung oder die Exposition sensibler Daten, und automatisierte Schutzmaßnahmen fangen die meisten Probleme ab. Kurz gesagt, die Organisation kann **die Intelligenz von Copilot mit Internetdaten erweitern, ohne die Kontrolle zu verlieren.**

3. Verhinderung von übermäßiger Freigabe und Datenverlust – Richtlinien für sichere Zusammenarbeit

Ein wesentliches Anliegen bei der unternehmensweiten Einführung von Copilot ist das Potenzial für die **übermäßige Freigabe sensibler Informationen**. Copilot generiert Inhalte (z. B. Zusammenfassungen, E-Mails, Dokumente) und kann auf riesige Mengen an Unternehmensdaten zugreifen, während er Benutzer unterstützt. Sitzung 3 konzentrierte sich darauf, sicherzustellen, dass diese Macht nicht zu versehentlichen Datenlecks oder Berechtigungsverletzungen führt. Im Wesentlichen befasste sich das Thema damit, wie man die „Copilot-gestützte Zusammenarbeit“ sicher hält und dabei die gleichen Datensicherheitsstandards wie bei traditionellen Arbeitsabläufen beibehält.

Bedeutung für Entscheidungsträger:

Datenschutz steht bei der Führungsebene an erster Stelle – eine einzige unbeabsichtigte Offenlegung vertraulicher Daten (z. B. das Teilen eines Finanzberichts mit allen Mitarbeitern mithilfe von Copilot) kann rechtliche und rufschädigende Konsequenzen haben. Diese Sitzung ist entscheidend, da sie die **Governance-Toolbox** zur Verhinderung solcher Vorfälle bereitstellt. Entscheidungsträger erhielten Einblicke in:

- Wie die Fähigkeit von Copilot, Informationen aus mehreren Quellen zu ziehen, **Daten preisgeben könnte, die Benutzer normalerweise nicht teilen würden**, wenn sie nicht richtig konfiguriert ist (z. B. das Einbeziehen einer vertraulichen Projektdatei in eine Antwort auf eine allgemeinere Frage).
- Die Notwendigkeit **konsistenter Zugriffskontrollen**: Copilot sollte einem Benutzer nur Inhalte zeigen, die er gemäß dem Berechtigungsmodell der Organisation sehen darf.
- Methoden, um **Copilot (und Benutzer) darüber aufzuklären**, welche Inhalte nicht geteilt oder sogar in Antworten verwendet werden dürfen (wie z. B. Entwürfe von Gewinn- und Verlustrechnungen, persönliche Identifikatoren usw.).

Kurz gesagt, dieses Thema hilft, **Vertrauen** zu wahren: Benutzer vertrauen darauf, dass Copilot keine „Geheimnisse ausplaudert“, und das Management vertraut darauf, dass die Organisation durch die Aktivierung von KI keinem höheren Risiko von Datenverlust ausgesetzt ist.

Herausforderungen:

Einige häufige Herausforderungen in diesem Bereich, die diskutiert wurden, umfassen:

- **Komplexe Berechtigungsumgebung:** Unternehmen haben oft kompliziert strukturierte Berechtigungen (SharePoint-Websites, Teams-Kanäle, Dateiberechtigungen). Copilot muss all diese respektieren. Eine Herausforderung besteht darin, zu überprüfen, ob „Vererbung“ und Ausnahmen bei Berechtigungen eingehalten werden. (Z. B. wird Copilot versehentlich eine Datei aus einem Team-Laufwerk verwenden, von dem jemand im Chat kein Mitglied ist?)
- **Unbeabsichtigtes Teilen durch Benutzer:** Benutzer erkennen möglicherweise nicht, dass ein Prompt wie „Teile Projektdetails von Foo mit dem Team“ ein sensibles Dokument oder eine Erkenntnis einbeziehen könnte. Traditionelle Werkzeuge verlassen sich darauf, dass Benutzer Inhalte manuell zum Teilen auswählen; mit Copilot könnten sie über natürliche Sprache teilen, ohne vollständig darüber nachzudenken.
- **Zonenbasierte Daten-Governance:** Viele Organisationen klassifizieren Daten nach Sensitivitäts-„Zonen“ (öffentlich, intern, vertraulich, streng vertraulich). Sicherzustellen, dass Copilot diese Kategorien richtig unterscheidet und handhabt, ist nicht trivial – es erfordert Planung und Konfiguration (z. B. welche SharePoint-Websites enthalten eingeschränkte Informationen? Benötigen diese zusätzliche Leitplanken?).
- **Mangelnde Sichtbarkeit von KI-Aktionen:** Anfangs könnten Manager Schwierigkeiten haben zu erkennen, was Copilot während seiner Unterstützung geteilt oder worauf er zugegriffen hat. Wenn ein Leck auftritt, können wir es überprüfen? Dies ist eine neue Herausforderung, die über die standardmäßigen Benutzeraktivitätsprotokolle hinausgeht.

Werkzeuge & Methoden:

Diese Sitzung stellte mehrere **greifbare Werkzeuge und Methoden** vor – viele davon von Microsoft Purview und SharePoint bereitgestellt –, um Risiken der übermäßigen Freigabe und des Datenverlusts zu mindern:

- **Data Loss Prevention (DLP)-Richtlinien für Copilot:** Erweiterung bestehender DLP-Regeln (die möglicherweise E-Mails oder Chat-Nachrichten mit sensiblen Informationen blockieren) auf die Ausgaben von Copilot. Zum Beispiel kann eine DLP-Regel erkennen, ob eine von Copilot generierte Nachricht oder Datei Kreditkartennummern oder andere regulierte Daten enthält, und **verhindern, dass sie geteilt oder sogar erstellt wird**. Diese Richtlinien können fein auf Copilot-Szenarien abgestimmt werden (wie das Scannen seiner Antworten in Echtzeit).

- **Vertraulichkeitsbezeichnungen und Co-Authoring-Kontrollen:** Durch die Anwendung von **Vertraulichkeitsbezeichnungen** (z. B. „Vertraulich“, „Streng vertraulich“) auf Dokumente und E-Mails ermöglichen Organisationen Copilot, Inhalte je nach Bezeichnung unterschiedlich zu behandeln. In der Praxis: Wenn ein Benutzer Copilot eine Frage stellt und ein relevantes Dokument als „Streng vertraulich“ gekennzeichnet ist, kann Copilot so konfiguriert werden, dass er es entweder aus der Antwort **ausschließt** oder es **einschließt, aber kennzeichnet**. Wenn Copilot geschützte Inhalte in eine Antwort aufnimmt, erbt diese Antwort die Bezeichnung (und wird automatisch als „Streng vertraulich“ gekennzeichnet). Dies wurde in der Veranstaltung gezeigt – Copilot weigerte sich, eine Datei mit der Bezeichnung „Projekt Obsidian – Vertraulich“ aufgrund der Richtlinie zusammenzufassen und schützte so den Inhalt.
- **SharePoint Advanced Management (SAM):** Dieses Set von Funktionen adressiert die übermäßige Freigabe an der Quelle (den Daten-Repositories, aus denen Copilot schöpft). Wichtige Funktionen sind:
    - **Berichte über Einblicke in die übermäßige Freigabe:** Administratoren können Berichte ausführen, um Dateien oder Websites mit falsch konfigurierten Berechtigungen (z. B. „Jeder“ hat Zugriff) zu finden. Durch deren Verschärfung verringern sie die Wahrscheinlichkeit, dass Copilot überhaupt auf etwas breit zugreifen kann.
    - **Automatische Zugriffsüberprüfungen:** SAM kann Website-Besitzer auffordern, regelmäßig zu bestätigen, wer Zugriff haben sollte. Dies schützt indirekt die Nutzung von Copilot – wenn weniger Personen Zugriff haben, können auch weniger Personen Copilot nach diesen Daten fragen.
    - **Restricted Access Control (RAC):** Eine drastische, aber nützliche Option – wenn ein besonders sensibles Projekt im Gange ist, kann eine Website in den „RAC-Modus“ versetzt werden, was bedeutet, dass Copilot sie als tabu behandelt, selbst wenn jemand Zugriff auf die Website hat (es sei denn, der Benutzer navigiert explizit im Kontext dorthin). Im Wesentlichen eine website-weite „Copilot nicht verwenden“-Kennzeichnung. Entscheidungsträger könnten dies beispielsweise während eines geheimen Fusions-/Übernahmeprojekts verwenden.
- **Copilot-spezifische Überwachung und Aufsicht:** Die Plattform bietet **Activity Explorer**-Protokolle, die die Aktivitäten von Copilot aufzeichnen (z. B. „Copilots von Benutzer X hat auf Datei Y um 10:00 Uhr zugegriffen“). Administratoren und Sicherheitsbeauftragte sollten diese wie andere Audit-Protokolle überwachen. Das **Insider Risk Management**-Modul von Purview kann Copilot-Aktivitäten mit anderen Verhaltensweisen korrelieren – zum Beispiel, wenn ein Mitarbeiter, der das Unternehmen verlässt, beginnt, Copilot nach vielen vertraulichen Daten zu

fragen, wird dieses Muster gekennzeichnet. (Dies wird im nächsten Abschnitt über Insider-Risiken erweitert.)

Diese Werkzeuge, zusammengefasst in Tabelle 3, bilden ein Sicherheitsnetz:

Tabelle 3. Wichtige Datenschutzwerkzeuge für Copilot

Werkzeug/Methode	Was es tut	Praktische Anwendung
Data Loss Prevention (DLP) für Copilot	Scannt die Ein-/Ausgaben von Copilot auf sensible Informationen (z. B. PCI, PII) und blockiert oder auditiert Regelverstöße.	Verhindert, dass definierte sensible Datentypen über Copilot geteilt werden. Z. B. Blockieren von Kreditkartennummern in Chats oder Dokumenten.
Vertraulichkeitsbezeichnungen & Inhaltskennzeichnung	Kennzeichnet Inhalte mit Vertraulichkeitsstufen; Copilot kann diese Bezeichnungen respektieren (zurückhalten oder gekennzeichnete Daten hervorheben).	Stellt sicher, dass nur angemessen freigegebene Informationen in Antworten verwendet werden. Z. B. keine „Streng vertraulichen“ Informationen in allgemeinen Antworten einschließen.
SharePoint-Berechtigungen & SAM-Bericht zur übermäßigen Freigabe	Identifiziert und korrigiert breit freigegebene Websites/Dateien (wie „Jeder“-Zugriff oder unterbrochene Vererbung, bei der Unterordner einen breiteren Zugriff haben als der übergeordnete Ordner).	Reduziert die Wahrscheinlichkeit eines unbeabsichtigten Zugriffs. Z. B. Entfernen der „Jeder“-Gruppe von einer Website, damit Copilot diesen Inhalt nicht für alle Benutzer verwenden kann.
Restricted Access Control (SharePoint SAM)	Sperrt vorübergehend eine sensible Website, sodass nur eine enge Whitelist (oder niemand) Copilot-Zugriff darauf hat.	In extremen Fällen sensible Projektdaten vor KI unter Quarantäne stellen. Z. B. wird eine streng geheime F&E-SharePoint-Website unter RAC gestellt, bis das Projekt abgeschlossen ist.

Copilot-Audit-Protokolle & Warnungen	Aufzeichnung, welche Informationen Copilot abgerufen oder bereitgestellt hat; Warnungen bei Richtlinienabweichungen.	Überwachen Sie ungewöhnliche Copilot-Nutzung. Z. B. Alarm, wenn Copilot Inhalte von einer Finanz-Website außerhalb der Geschäftszeiten zurückgibt (potenzielles Data-Mining).

Durch die Kombination dieser Maßnahmen schaffen Entscheidungsträger eine robuste Umgebung, in der **Mitarbeiter frei mit Copilot zusammenarbeiten können, ohne Angst vor versehentlichen Lecks**. Zum Beispiel kann ein HR-Direktor sicher eine Vorlage für ein Angebotsschreiben mit Copilot erstellen, die auf früheren Angeboten basiert, in dem Wissen, dass alle persönlichen Gehaltsdaten durch Bezeichnungen und DLP geschützt sind. Das Copilot-Kontrollsystem fügt im Wesentlichen eine „KI-Sicherheitsschicht“ über die traditionelle Datensicherheit.

Best Practices:

- **Least-Privilege-Datenzugriff:** Stellen Sie sicher, dass die Datenkonnektoren von Copilot (SharePoint, Teams usw.) mit den eigenen Berechtigungen jedes Benutzers ausgeführt werden. Auf diese Weise wird Copilot eine Datei, die ein Benutzer normalerweise nicht sehen darf, auch nicht anzeigen. (Standardmäßig folgt Copilot diesem Modell.) Es lohnt sich, dass die IT überprüft, ob Integrationen oder Drittanbieter-Konnektoren diese Regel beibehalten.
- **Regelmäßige Überprüfungen von Copilot-Antworten:** Besonders während der Einführung ist es ratsam, einen Champion oder Administrator regelmäßig Stichproben der Copilot-Ausgaben zu nehmen, um zu sehen, ob sensible Informationen durchrutschen. Wenn etwas entdeckt wird, passen Sie sofort die DLP- oder Kennzeichnungsrichtlinien an und verwenden Sie diesen Vorfall als Schulungsbeispiel.
- **Benutzerschulung zur Datenhandhabung:** Betonen Sie den Benutzern, dass **Copilot eine Erweiterung ihrer selbst** in Bezug auf den Datenzugriff ist. Sie sollten seine Vorschläge oder zusammengestellten Inhalte mit der gleichen Sorgfalt behandeln, als hätten sie sie manuell zusammengestellt. Wenn Copilot beispielsweise eine vertrauliche Datei für sie zusammenfasst, sollten sie diese Zusammenfassung auch nicht in einen öffentlichen Chat einfügen. Erinnern Sie sie: **„Wenn Sie die Datei nicht teilen können, teilen Sie auch die Antwort von Copilot nicht.“**

Durch proaktives Management dieser Risiken können Organisationen die Effizienz von Copilot in der täglichen Teamarbeit selbstbewusst nutzen und gleichzeitig eine **feste Kontrolle über die Daten-Governance** behalten.

4. Insider-Risikomanagement – Erkennung und Minderung des Missbrauchs von Copilot

Während sich der vorherige Abschnitt mit versehentlicher Datenexposition befasste, behandelte diese Sitzung ein schwierigeres Szenario: **Insider-Risiken**. Dies bezieht sich auf Situationen, in denen ein Benutzer – absichtlich oder unabsichtlich – Copilot auf eine Weise verwendet, die der Organisation schaden könnte, z. B. durch den Versuch, sensible Informationen zu extrahieren, die er nicht haben sollte, oder durch Handlungen, die gegen Richtlinien verstoßen. Copilot schafft keine neuen Insider-Bedrohungen, aber wie jedes leistungsstarke Werkzeug könnte er von einem **böswilligen Insider (der absichtlich handelt)** oder einem **fahrlässigen Insider (der unachtsam handelt)** missbraucht werden. Entscheidungsträger müssen darauf vorbereitet sein, solchen Missbrauch schnell zu erkennen und zu stoppen.

Bedeutung für Entscheidungsträger:

Insider-Vorfälle gehören zu den schädlichsten Sicherheitsereignissen (z. B. ein Mitarbeiter, der eine Kundenliste herunterlädt, bevor er zu einem Konkurrenten wechselt). Die Geschwindigkeit und Reichweite von Copilot könnten die Fähigkeit eines Insiders, Informationen zu sammeln, verstärken. Für die Führungsebene ist es entscheidend zu wissen, dass die Einführung von Copilot ihr Sicherheitsteam nicht **überrumpeln** wird – tatsächlich kann das Kontrollsystem von Copilot, wie in dieser Sitzung vorgestellt, Insider-Risikoprogramme mit KI-spezifischen Signalen erweitern. Wichtige Gründe, warum dies von Bedeutung ist:

- **Schutz sensibler Vermögenswerte:** Wenn jemand versucht, Daten über Copilot abzuschöpfen (z. B. durch eine Reihe von Fragen, um ein Geheimnis zusammenzusetzen), muss die Organisation dies wissen und eingreifen.
- **Aufrechterhaltung von Compliance und ethischer Nutzung:** Entscheidungsträger sind dafür verantwortlich sicherzustellen, dass KI-Werkzeuge intern nicht für unethische oder illegale Zwecke verwendet werden (z. B. zur Erstellung unangemessener Inhalte oder zur Belästigung mittels KI in der Kommunikation).
- **Benutzerverantwortlichkeit:** Mitarbeiter sollten verstehen, dass Copilot-Aktivitäten angemessen überwacht werden – diese Abschreckung entmutigt tatsächlich den vorsätzlichen Missbrauch. Umgekehrt schützt es auch Mitarbeiter, indem es erkennt, ob vielleicht ihr Konto kompromittiert wurde und jemand anderes Copilot über ihren Zugang nutzt (ein Szenario mit einem externen Akteur).

Herausforderungen:

Das Management von Insider-Risiken im Kontext von Copilot bringt einige neue Aspekte mit sich:

- **Volumen der Interaktionen:** Copilot kann in kurzer Zeit viele Aktionen oder Datenabrufe durchführen (er könnte Dutzende von Fragen in Minuten beantworten). Traditionelle Warnungen (wie „100 Dateien heruntergeladen“) müssen möglicherweise neu kalibriert werden – z. B. könnte „Copilot hat 100 Dateien für Benutzer X in einer Stunde aufgerufen“ je nach Kontext normal für Recherchen oder alarmierend sein. Die Unterscheidung zwischen gutartiger hoher Nutzung und böswilliger Aktivität kann eine Herausforderung sein.
- **Unauffälligere Datensammlung:** Ein versierter Insider könnte versuchen, Daten zu erhalten, ohne offensichtliche Alarme auszulösen – anstatt Dateien herunterzuladen, könnte er Copilot auffordern, Schlüsselpunkte aus sensiblen Dokumenten zusammenzufassen oder aufzulisten, und so unter dem Radar des Dateizugriffs fliegen.
- **Mehrere kleine Vorfälle, die ein Muster bilden:** Eine einzelne sensible Frage eines Mitarbeiters an Copilot mag harmlos sein. Aber wenn er über einen Monat hinweg systematisch eine Reihe von vertraulichen Themen abfragt, deutet dieses Muster auf ein Risiko hin. Das Erkennen von Mustern über Zeit und Datenquellen hinweg ist eine Komplexität, die wie geschaffen für die KI-Analyse ist.
- **Falsch-Positive vs. Negative:** Das System so abzustimmen, dass es nicht ständig falschen Alarm schlägt (z. B. einen Finanzanalysten markiert, der Copilot vor den Quartalsergebnissen intensiv nutzt), aber auch keine echten roten Flaggen übersieht (ein Ingenieur, der normalerweise nie Finanzdaten anfasst, fragt plötzlich Umsatzzahlen über Copilot ab).

Werkzeuge & Methoden:

Die Sitzung zeigte, wie die **Insider Risk Management (IRM)**-Lösung von Microsoft Purview erweitert wurde, um Copilot-Aktivitäten abzudecken. Hier sind die wichtigsten Werkzeuge und Methoden, die Entscheidungsträgern und ihren Sicherheitsteams zur Verfügung stehen:

- **Insider-Risikorichtlinien für die KI-Nutzung:** Administratoren können Risikobewertungsregeln definieren, die Copilot-Signale enthalten. Zum Beispiel kann eine IRM-Richtlinie so festgelegt werden: „Wenn ein Benutzer, der die Organisation in <30 Tagen verlässt (erkannt durch ein HR-Austrittskennzeichen), plötzlich beginnt, über Copilot auf ein hohes Volumen vertraulicher Dateien zuzugreifen, als hohes Risiko kennzeichnen.“ Dies verbindet HR-Daten, Dateizugriffsprotokolle und Copilot-Aktivitäten zu einem einzigen Risikoscore.

- **Automatisierte Sequenzerkennung:** Das System (mit maschinellem Lernen) sucht nach Aktionssequenzen, die zusammen auf einen potenziellen Vorfall hindeuten. In der Demo sahen wir ein Szenario: *Benutzer fragt Copilot nach sensiblen Daten → Copilot produziert als vertraulich gekennzeichneten Inhalt → Benutzer lädt dann referenzierte Dateien herunter*. Einzeln mag jeder Schritt erlaubt sein; zusammen bilden sie eine Eskalationskette. Purview kann diese mehrstufigen Sequenzen erfassen und eine Warnung generieren, dass „Benutzer X möglicherweise versucht, sensible Informationen mit Copilot zu exfiltrieren."
- **Adaptive Protection (Dynamische Richtlinienanpassung):** Vielleicht der innovativste Teil – sobald ein Benutzer als Insider-Risiko identifiziert ist, können bestimmte Kontrollen für diesen Benutzer automatisch verschärft werden. Wenn beispielsweise Benutzer Y mehrere Warnungen auslöst und nun als „Hohes Risiko" eingestuft wird, kann das System automatisch verhindern, dass Copilot die sensiblen Anfragen dieses Benutzers überhaupt beantwortet (die Veranstaltung beschrieb ein Beispiel: eine Richtlinie kann den Status eines Benutzers so ändern, dass jeder Versuch, Copilot für geschützte Dateien zu verwenden, direkt blockiert und nicht nur überwacht wird). Im Wesentlichen **ändert der Risikoscore des Benutzers seine Berechtigungen in nahezu Echtzeit**. Dieser adaptive Ansatz bedeutet, dass Sie nicht jeden mit superstrengen Einstellungen bestrafen – die meisten Benutzer arbeiten normal, aber der Copilot-Zugriff eines markierten Benutzers kann leise gedrosselt oder eingeschränkt werden.
- **Kommunikationsüberwachung für Copilot-Missbrauch:** Wenn ein Insider versucht, Copilot zur Erstellung unangemessener Kommunikation (z. B. beleidigende Inhalte oder Belästigung) zu verwenden, kommt **Communication Compliance** ins Spiel. Es gibt maschinelle Lernklassifikatoren, die von Copilot generierte Nachrichten oder E-Mails lesen können, um Toxizität oder sensible Inhalte zu erkennen. Die Sitzung gab ein interessantes Beispiel: **Prompt-Injection-Angriffe**. Wenn ein Benutzer versucht, Copilot anzuweisen, Richtlinien zu ignorieren oder unzulässige Ausgaben zu produzieren (eine Art von Missbrauch), kann das System diesen Versuch in nahezu Echtzeit erkennen und blockieren. Aus Sicht eines Entscheidungsträgers ist dies eine Zusicherung, dass Mitarbeiter nicht einfach clevere Tricks anwenden können, um die Sicherheitsregeln von Copilot zu untergraben – und dass solche Versuche als Richtlinienverstöße protokolliert werden.

In der Praxis sollten Sicherheitsteams diese KI-spezifischen Werkzeuge in ihre bestehenden Insider-Risiko-Workflows integrieren:

- **Regelmäßige Risiko-Überprüfungsmeetings:** So wie Sicherheitsteams täglich/wöchentlich DLP-Vorfälle oder Kontosperrungen überprüfen, werden sie

nun auch Copilot-Vorfallsberichte einbeziehen. Erwarten Sie neue Vorfallstypen wie „Versuchter sensibler Datenabgriff über Copilot“ auf der Tagesordnung.

- **Eskalationsprotokoll:** Wenn eine Insider-Risikowarnung aus der Copilot-Nutzung einen bestimmten Schwellenwert überschreitet (z. B. vom System als „Hohe Schwere“ eingestuft), könnte dies sofortige Maßnahmen auslösen – wie die vorübergehende Sperrung des Copilot-Zugriffs des Benutzers (was über ein Kennzeichen in seinem Benutzerprofil oder durch adaptive Richtlinien, wie erwähnt, erfolgen kann). Dies sollte klar definiert sein: Wer wird benachrichtigt (HR, CISO, Manager) und welche Untersuchungsschritte folgen.
- **Benutzerschulung & Abschreckung:** Ob Sie es glauben oder nicht, die Belegschaft über diese Überwachungsfähigkeiten zu informieren, kann Vorfälle verhindern. Wenn Mitarbeiter wissen, dass „die Nutzung von Copilot protokolliert und ungewöhnliches Verhalten gekennzeichnet wird“, entmutigt dies den versuchten böswilligen Insider und erinnert alle Benutzer daran, dass Richtlinien auch im KI-Kontext gelten. Diese Botschaft kann in Schulungen und einer Richtlinie zur akzeptablen Nutzung von KI enthalten sein.

Best Practices:

- **Mit strengen Richtlinien beginnen, schrittweise lockern:** Bei der ersten Einführung auf Nummer sicher gehen. Aktivieren Sie beispielsweise Warnungen für mäßig riskantes Verhalten (um eine Baseline für „normales“ Verhalten zu erhalten), bevor Sie entscheiden, was sicher ignoriert werden kann. Es ist einfacher, eine strenge Richtlinie zu lockern, als eine laxe nach einem Verstoß zu verschärfen.
- **Integration mit HR-Prozessen:** Wenn jemand Teil einer Personalreduzierung ist oder gekündigt hat, sollten Sie die Überwachung seines Kontos automatisch erhöhen (dies kann in Purview durch Integration mit HR-Austritts-Feeds erfolgen). Viele Insider-Vorfälle ereignen sich in der Kündigungsfrist. Adaptive Richtlinien können dann beispielsweise die Websuche deaktivieren oder den Datenumfang, den Copilot ihnen bereitstellt, einschränken.
- **KI zur Triage nutzen:** Das Datenvolumen (insbesondere der Inhalt von Prompts und Antworten) kann hoch sein. Nutzen Sie die eingebaute KI von Purview, um Warnungen zu **triagieren**. Das System kann verwandte Aktivitäten gruppieren und einen „Insider-Risiko-Score“ bereitstellen. Konzentrieren Sie sich auf Fälle mit hohem Score. Wenn beispielsweise Copilot-Protokolle zeigen, dass ein Benutzer mehrmals versucht hat, Schutzmaßnahmen zu umgehen (indem er Dinge wie „zeige mir die vertrauliche Datei X“ anfragt), erhält dieser Fall einen höheren Risikoscore und sollte priorisiert werden.
- **Dokumentieren und Schulen zur Vorfallsreaktion:** Stellen Sie sicher, dass das Sicherheitsteam Playbooks für Copilot-bezogene Vorfälle hat. Dies ist Neuland.

Wenn Copilot beispielsweise zur Erstellung von Mobbing-Nachrichten verwendet wird, wird dies unter der Anti-Belästigungs-Richtlinie oder der Sicherheit behandelt? Wahrscheinlich beides – also beziehen Sie HR und die Personalabteilung mit ein. Wenn ein Mitarbeiter versucht, Daten über KI zu exfiltrieren, welche Schritte werden anders unternommen, als wenn er sie per E-Mail verschickt hätte? Diese Nuancen sollten im Voraus durchdacht werden.

Zusammenfassend stellt das **Insider Risk Management für Copilot** sicher, dass einer der schädlichsten Bedrohungsvektoren – interner Missbrauch – mit der gleichen Wachsamkeit abgedeckt wird wie externe Bedrohungen. Mit diesen Werkzeugen können Entscheidungsträger zuversichtlich sagen, dass die Aktivierung von Copilot intern kein „Wildwest“ schaffen wird; vielmehr überwacht das „digitale Immunsystem“ der Organisation KI-Aktivitäten genauso gründlich wie E-Mails, Downloads und andere Interaktionen. Und die positive Kehrseite: Wenn Missbrauch praktisch unmöglich oder schnell aufgedeckt wird, kann jeder andere Copilot frei nutzen, um zu innovieren, ohne dass ein paar schwarze Schafe den Spaß verderben.

5. Copilot-Nutzungsanalysen und ROI – Messung von Auswirkungen und Erfolgskennzahlen

Nachdem Governance- und Sicherheitskontrollen behandelt wurden, verlagert sich der Fokus auf die **Wertrealisierung**. In dieser Sitzung ging es darum, zu messen, wie Copilot und KI-Agenten genutzt werden und ob sie die versprochenen Produktivitätsvorteile liefern. Für Entscheidungsträger (insbesondere Business-Sponsoren und IT-Leiter) ist es entscheidend, **harte Daten** zu haben, die beantworten: Macht Copilot einen Unterschied? Wenn ja, wie können wir das quantifizieren? Wenn nicht vollständig, wo gibt es Lücken, um die Akzeptanz oder den Nutzen zu verbessern?

Bedeutung für Entscheidungsträger:

Die Investition in Copilot (durch Lizenzierung, Integrationsarbeit, Benutzerschulung) stellt ein erhebliches Engagement dar. Entscheidungsträger müssen diese Investition durch **konkrete Metriken** rechtfertigen. Darüber hinaus ermöglicht eine kontinuierliche Messung datengesteuerte Entscheidungen: die Ausweitung von Copilot auf mehr Benutzer, die Fokussierung von Schulungen auf wenig genutzte Funktionen oder die Anpassung von Konfigurationen. Diese Sitzung demonstrierte, dass **„man nicht managen kann, was man nicht misst."** Wichtige Punkte:

- **Akzeptanzverfolgung:** Einfach ausgedrückt, nutzen die Mitarbeiter Copilot? Zum Beispiel, welcher Prozentsatz der lizenzierten Benutzer ruft Copilot wöchentlich aktiv auf? Wenn die Nutzung gering ist, muss die Führung untersuchen, warum (Bewusstsein? Nützlichkeit? Zugangsprobleme?) und korrigierende Maßnahmen ergreifen (vielleicht mehr Schulungen oder Funktionsanpassungen).
- **Produktivitäts- und Effizienzmetriken:** Über die reine Nutzung hinaus, wie beeinflusst Copilot die Arbeitsergebnisse? Wenn beispielsweise das Erstellen eines Projektupdates vor Copilot 2 Stunden dauerte und jetzt 1 Stunde, ist das eine messbare Effizienzsteigerung. Skaliert über viele Aufgaben und Mitarbeiter, veranschaulichen diese Einsparungen den ROI in Zeit (und damit Kosten). Entscheidungsträger wollen diese Aggregationen sehen – „Copilot hat in diesem Quartal X Stunden Zeit gespart" oder „Die Copilot-Akzeptanz korreliert mit einer 15 % schnelleren Falllösung im Kundensupport."
- **Benutzerzufriedenheit und Qualität:** Sind die Benutzer mit den Antworten von Copilot zufrieden? Wenn sie die Hälfte der Vorschläge als irrelevant empfinden und die Arbeit neu machen müssen, sinkt der ROI. Daher ist die Verfolgung qualitativen Feedbacks (über Umfragen oder Bewertungen) wichtig. Auch die **wiederholte Nutzung** ist ein Indikator: Wenn die Leute täglich zurückkommen, um es zu nutzen, bietet es einen wahrgenommenen Wert, während ein

Werkzeug, das einmal verwendet und dann aufgegeben wird, auf Probleme hinweist.

- **Identifizierung von hochwertigen Anwendungsfällen:** Analysen können aufzeigen, welche Copilot-Funktionen oder Anwendungsfälle am beliebtesten oder effektivsten sind. Zum Beispiel könnten Analysen zeigen, dass 80 % der Copilot-Interaktionen darin bestehen, dass Leute lange Dokumente zusammenfassen lassen. Diese Erkenntnis sagt Entscheidungsträgern a) dass diese Funktion extrem wertvoll ist – vielleicht mehr darin investieren, und b) andere Funktionen werden zu wenig genutzt – vielleicht brauchen sie Förderung oder sind nicht so nützlich. Dies leitet die zukünftige Entwicklung und die Prioritäten der Schulung.

Herausforderungen:

Die genaue Messung der Auswirkungen hat einige Herausforderungen:

- **Zuschreibung von Produktivitätsgewinnen:** Es ist von Natur aus schwierig zu beweisen, dass ein Dokument, bei dessen Erstellung Copilot geholfen hat, die Hälfte der Zeit in Anspruch nahm. Wir verlassen uns oft auf Selbstauskünfte der Benutzer oder Annäherungen (wie die Anzahl der von Copilot generierten Wörter im Vergleich zu manuell erstellten). Während der Sitzung diskutierten die Präsentatoren Metriken wie „von Copilot unterstützte gesparte Stunden“, die Schätzungen sind, die auf Annahmen basieren (jede Copilot-Aktion = X gesparte Minuten). Entscheidungsträger sollten verstehen, dass dies Schätzungen sind, wenn auch fundierte.
- **Datenüberflutung:** Die Analysesysteme generieren eine Menge Daten – Nutzung nach Benutzer, nach Funktion, nach Stunde. Die Herausforderung besteht darin, **aussagekräftige KPIs** zu extrahieren, die mit den Geschäftsergebnissen übereinstimmen. Es ist leicht, in Diagrammen zu ertrinken. Man muss sich auf eine Handvoll **Key Performance Indicators (KPIs)** für die regelmäßige Berichterstattung an die Führungsebene einigen (Beispiele: wöchentlich aktive Copilot-Benutzer, durchschnittliche Copilot-Interaktionen pro Benutzer pro Tag, von Benutzern gemeldete oder berechnete Zeitersparnis, Reduzierung des Support-Ticket-Backlogs, wenn Copilot im Self-Service verwendet wird usw.).
- **ROI in finanzieller Hinsicht:** Die Übersetzung von Effizienz in Dollar-Einsparungen oder Umsatzsteigerungen kann umstritten sein. Zum Beispiel bedeutet gesparte Zeit nicht immer gespartes Geld, es sei denn, man reduziert Überstunden oder setzt Personal neu ein. Führungskräfte könnten die ROI-Zahlen in Frage stellen – „Zeigen Sie mir, wie diese gesparte Zeit das Endergebnis verbessert hat.“ Dies erfordert die Verknüpfung von Copilot-Metriken mit Geschäftsmetriken (z. B. könnten schnellere Verkaufsangebote zu

mehr eingereichten Geboten führen, was mehr Gewinne bedeuten könnte). Diese Analyse kann kompliziert sein und einen längeren Beobachtungszeitraum erfordern.

- **Gewährleistung des Datenschutzes in der Analytik:** Ironischerweise muss man bei der Messung der Nutzung darauf achten, die Privatsphäre nicht zu verletzen. Die Analytik sollte sich auf aggregierte Trends konzentrieren, nicht auf die Überwachung des Inhalts einzelner Personen. Aus Vertrauensgründen anonymisieren oder aggregieren Organisationen oft Copilot-Nutzungsdaten, wenn sie diese breit teilen.

Werkzeuge & Methoden:

Die Sitzung demonstrierte die integrierten Analyse- und Berichtswerkzeuge von Microsoft für Copilot, die das Sammeln und Interpretieren dieser Metriken erleichtern:

- **CoPilot Usage Dashboard (Microsoft 365 Admin Center):** Ein vorgefertigtes Dashboard, das Akzeptanz- und Nutzungstrends anzeigt. Es enthält typischerweise:
    - **Aktive Benutzer:** Wie viele Benutzer haben in den letzten Tag/Woche/Monat mit Copilot interagiert.
    - **Nutzungsintensität:** Zum Beispiel die durchschnittliche Anzahl der Copilot-Aktionen pro Benutzer pro Tag. Dies hilft zu erkennen, ob es sich um eine einmalige Neuheit oder ein tief verankertes Werkzeug handelt.
    - **Aufschlüsselung der Funktionsnutzung:** Z. B. 40 % der Copilot-Anfragen betreffen das Entwerfen von E-Mails, 30 % die Zusammenfassung von Dokumenten, 20 % die Datenanalyse, 10 % Sonstiges. (Diese Zahlen sind hypothetisch, aber solche Aufschlüsselungen wurden als verfügbar erwähnt.)
    - **Web- vs. Arbeitsdatennutzung:** Zeigt vielleicht, wie oft Copilot das Web im Vergleich zu nur internen Daten abfragt, was auf die Abhängigkeit von Internetinformationen hinweist.
    - **CoPilot Assisted Hours Saved:** Wie in der Veranstaltung gezeigt, hat Microsoft eine Metrik, die die Anzahl bestimmter Aktionen mit einer geschätzten Zeitersparnis pro Aktion multipliziert, um die gesparten Stunden zu quantifizieren. Entscheidungsträger können dies als richtungsweisenden Indikator für Produktivitätsgewinne verwenden.
- **Viva Insights & Custom Analytics:** Für eine maßgeschneiderte Analyse können Entscheidungsträger auf Viva Insights zurückgreifen (das jetzt benutzerdefinierte Daten wie die Copilot-Nutzung akzeptiert). Man könnte beispielsweise die **in Meetings verbrachte Zeit oder die Arbeitsbelastung nach Feierabend** vor und nach der Einführung von Copilot für bestimmte Teams vergleichen – ein

Rückgang könnte darauf hindeuten, dass Copilot hilft, die Arbeit schneller während der normalen Arbeitszeit zu erledigen. Darüber hinaus kann man durch das Hochladen von Geschäftsergebnisdaten (Verkaufszahlen, Support-Lösungszeiten) und deren Korrelation mit der Copilot-Nutzung (wie es Mikes Team tat) nach Mustern wie „Teams, die Copilot intensiv nutzen, zeigen 10 % kürzere Verkaufszyklen“ suchen. Dies erfordert statistische Analysen und wurde als fortgeschrittener Schritt zur Messung der Auswirkungen (nicht nur der Nutzung) erwähnt.

- **Periodische Benutzerumfragen (CoPilot „Pulse Checks“):** Eine einfache, aber effektive Methode: Nach einigen Wochen der Nutzung befragen Sie Ihre Benutzerbasis mit ein paar Fragen: „Auf einer Skala von 1-5, wie viel Zeit glauben Sie, spart Ihnen Copilot pro Woche?“, „Nennen Sie eine Aufgabe, die Copilot einfacher gemacht hat, und eine, bei der er nicht geholfen hat.“ Diese qualitativen Eingaben geben den Zahlen Kontext und können Erfolgsgeschichten oder Schmerzpunkte aufzeigen. Oft können diese Anekdoten (z. B. „Die Besprechungszusammenfassungen von Copilot geben mir die Freiheit, mich auf die Diskussion zu konzentrieren, anstatt Notizen zu machen“) in Berichte aufgenommen werden, um den Statistiken Farbe zu verleihen.
- **Definition von Key Performance Indicators (KPIs):** Basierend auf dem oben Genannten sollte die Führung einen Kernsatz von KPIs festlegen, die regelmäßig überwacht werden. Tabelle 4 bietet ein Beispiel-KPI-Set, das monatlich an die Stakeholder berichtet werden könnte:

Tabelle 4. Beispiel-KPIs für die Wertrealisierung von Copilot

KPI	Beschreibung	Ziel/Benchmark
Aktive Copilot-Benutzerrate	% der lizenzierten Benutzer, die Copilot in den letzten 7 Tagen mindestens 1x verwendet haben. (Akzeptanzindikator)	z. B. 75 % nach 3 Monaten der Einführung.
Durchschnittliche tägliche Interaktionen pro Benutzer	Wie viele Prompts oder Aktionen der typische aktive Benutzer pro Tag generiert. (Engagement-Tiefe)	Baseline bei Einführung; Ziel, um 20 % über 2 Monate zu steigern.
Benutzerzufriedenheits-Score (CoPilot)	Durchschnittliche Bewertung aus einer Benutzerumfrage (z. B. „Wie hilfreich ist Copilot insgesamt für	z. B. ≥4,0/5,0 im Durchschnitt nach 1 Quartal.

	Ihre Arbeit?“ auf einer 5-Punkte-Skala).	
Geschätzte Zeitersparnis (Stunden/Benutzer/Woche)	Aggregierte Messung aus der Nutzungstelemetrie, die Copilot-Ausgaben in gesparte Zeit umrechnet.	z. B. 3 Stunden pro Benutzer pro Woche (Ziel).
Aufgabenbeschleunigung	Spezifische Aufgabenmetrik – z. B. Zykluszeit für Verkaufsangebote oder Lösungszeit für Support-Tickets, im Vergleich vor/nach Copilot.	z. B. -15 % schnellere Lösungszeit nach 6 Monaten.
Copilot-Antworten mit sensiblem Inhalt (überwacht)	Anzahl der Male, die Copilot versucht hat, geschützte Informationen anzuzeigen (sollte idealerweise aufgrund guter Richtlinien sinken).	Kein Ziel (weniger ist besser); zur Sicherstellung der Sicherheitseffizienz verwenden.

- **Regelmäßige ROI-Berichterstattung:** Schließlich verwenden Sie diese KPIs, um einen prägnanten monatlichen oder vierteljährlichen „Copilot Impact Report“ für Führungskräfte zu erstellen. Dieser Bericht könnte beispielsweise zeigen: „800 Mitarbeiter nutzen Copilot jede Woche aktiv und durchschnittlich 5 Mal pro Tag. Wir schätzen die Zeitersparnis im 3. Quartal auf ~12.000 Stunden im gesamten Unternehmen, was ungefähr X $ an Produktivität entspricht. Die Zufriedenheit ist hoch (4,2/5), und die Support-Tickets im Zusammenhang mit Copilot sind nach zusätzlichen Schulungen um 30 % gesunken, was auf eine wachsende Kompetenz hindeutet.“ Eine kurze Erzählung wie diese verwandelt Rohdaten in eine Geschäftsgeschichte.

Best Practices:

- **Kombinieren Sie quantitative und qualitative Daten:** Verlassen Sie sich nicht auf eine einzige Metrik. Wenn die Nutzung hoch, aber die Zufriedenheit niedrig ist, untersuchen Sie, warum (vielleicht sind die Leute gezwungen, es zu benutzen, finden es aber nicht hilfreich). Wenn die Zufriedenheit hoch, aber die Nutzung niedrig ist, liebt es vielleicht eine kleinere Gruppe – finden Sie heraus, wie Sie diesen Erfolg auf mehr Benutzer ausweiten können.
- **Benchmarken und Trends verfolgen:** Messen Sie nach Möglichkeit vor der Einführung (z. B. wie lange dauert es, einen Monatsbericht vor Copilot zu erstellen). Diese Benchmarks machen Verbesserungen deutlich. Verfolgen Sie auch die Trends von Monat zu Monat – ein Plateau oder ein Rückgang könnte

bedeuten, dass es Zeit ist, einzugreifen (durch mehr Schulungen oder neue Anwendungsfälle, um das Interesse aufrechtzuerhalten).

- **Champions für Einblicke einbeziehen:** Ihre Champion-Benutzer können Kontext zu den Metriken liefern. Zum Beispiel könnten Analysen eine geringe Nutzung in einer bestimmten Abteilung zeigen. Ein Champion dort könnte erklären: „Unsere Arbeit umfasst viel spezialisierte Software, mit der Copilot noch nicht integriert ist“, was Integrationspläne oder das Management der Erwartungen an den ROI dieser Abteilung beeinflussen könnte.
- **Erfolge veröffentlichen:** Wenn Analysen einen klaren Gewinn zeigen (sagen wir, ein Team hat ein Projekt dank Copilot in Rekordzeit abgeschlossen), veröffentlichen Sie dies intern. Dies rechtfertigt nicht nur die Investition nach oben, sondern fördert auch eine breitere Akzeptanz (FOMO – die Angst, diese Vorteile zu verpassen – kann ein großartiger Akzeptanztreiber unter Kollegen sein).

Durch die sorgfältige Analyse von Nutzung und Ergebnissen können Entscheidungsträger sicherstellen, dass Copilot nicht nur „gut klingt“, sondern **greifbaren Wert liefert**. Die Daten werden aufzeigen, wo es gut funktioniert und wo Kurskorrekturen erforderlich sind, sodass die Organisation kontinuierlich optimieren kann, wie Copilot eingesetzt wird. Im Wesentlichen schließt die Messung den Kreislauf des Copilot-Kontrollsystems: Sie sichern es, Sie verwalten es, die Leute nutzen es – dann **messen Sie es**, um Erkenntnisse zur Verbesserung der Sicherheits- und Verwaltungsentscheidungen zurückzugewinnen und den Erfolg zu demonstrieren.

6. Lebenszyklusmanagement von Agenten – Steuerung von KI-Agenten von der Erstellung bis zur Bereitstellung

Über den Kern-Copilot-Assistenten hinaus, der in Apps wie Teams und Outlook lebt, werden viele Organisationen benutzerdefinierte KI-**„Agenten“** entwickeln – spezialisierte Copilot-ähnliche Bots oder Assistenten, die auf bestimmte Abteilungen oder Funktionen zugeschnitten sind. Beispiele könnten ein **Sales CoPilot** sein, der Ihr CRM-System kennt, oder ein **HR Answer Bot**, den Mitarbeiter für HR-Fragen nutzen. Diese Agenten werden mit Copilot Studio und der Power Platform erstellt, oft von **„Makern“** innerhalb der Geschäftsbereiche (Power-User oder Citizen Developer) anstatt von professionellen Programmierern. Sitzung 6 befasste sich damit, wie der **Lebenszyklus dieser Agenten** verwaltet wird – von der ersten Experimentierphase des Makers bis zur unternehmensweiten Bereitstellung und Wartung.

Bedeutung für Entscheidungsträger:

Hier trifft KI-Innovation auf IT-Governance. Führungskräfte möchten Geschäftsbereiche befähigen, ihre eigenen Probleme mit KI zu lösen (es ist schneller, und die Personen, die dem Problem am nächsten sind, entwerfen oft die beste Lösung). Aber ohne Leitplanken könnten Hunderte von inoffiziellen Bots auftauchen, was zu inkonsistenter Qualität oder sogar Sicherheitslücken führen kann. Ein ordnungsgemäßes Lebenszyklusmanagement liefert:

- **Innovation im großen Maßstab, sicher:** Das Ziel ist, tausend Agenten blühen zu lassen – aber sicherzustellen, dass sie in den richtigen Gärten blühen (geeignete Umgebungen) und dass die besten für den unternehmensweiten Einsatz geerntet werden können.
- **Qualitätskontrolle:** Nicht jeder Prototyp-Agent sollte unternehmensweit verfügbar sein. Entscheidungsträger benötigen einen Trichter, um zu identifizieren, welche Bots Standards (Genauigkeit, Compliance) erfüllen, bevor sie breiter freigegeben werden.
- **Kosten- und Ressourcenmanagement:** Jeder Agent verbraucht Ressourcen (API-Aufrufe, Wartungsaufwand). Ein Lebenszyklusprozess verhindert Redundanz (10 Teams bauen denselben Bot, ohne voneinander zu wissen) und stellt sicher, dass ungenutzte Agenten außer Betrieb genommen werden. Dies optimiert Ausgaben und Aufwand.
- **Change Management:** Wenn sich Agenten weiterentwickeln (neue Funktionen, aktualisierte Datenquellen), sollte es eine Versionskontrolle und Tests geben – die Teil der Lebenszyklus-Governance sind. Dies stellt sicher, dass Updates für

einen weit verbreiteten Sales Bot beispielsweise die Funktionalität nicht unerwartet beeinträchtigen.

Herausforderungen:

Die Implementierung einer gut gesteuerten Maker-Kultur bringt mehrere Herausforderungen mit sich:

- **Balance zwischen Freiheit und Kontrolle:** Wenn die IT alles sperrt (niemand kann einen Agenten ohne Antrag erstellen), verlangsamt sich die Innovation und Schatten-IT kann aufblühen. Wenn die IT sich zurückhält, könnte ein „Wilder Westen“ von Bots entstehen, von denen einige potenziell unsicher oder fehlerhaft sind. Das richtige Gleichgewicht zu finden – oft durch eine **gestufte Umgebungsstrategie** – ist knifflig, aber entscheidend.
- **Umgebungs-Wildwuchs:** Mit vielen Makern kann es zu einer Explosion von Entwicklungsumgebungen, Testversionen und Duplikaten kommen. Administratoren benötigen Möglichkeiten, um Sichtbarkeit über all diese Agenten und ihre Standorte zu erhalten. Die Sitzung beschrieb neue Funktionen im **Power Platform Admin Center**, um alle Agenten über Umgebungen hinweg aufzulisten und zu überwachen – deren Einführung ist der Schlüssel, erfordert aber Bewusstsein und neue Prozesse auf der Admin-Seite.
- **Promotionspfad von Persönlich zu Produktion:** Viele großartige Lösungen beginnen als schneller persönlicher Bot. Die Herausforderung besteht darin, einen klaren Weg zu schaffen, um diesen Bot in eine **Produktionsumgebung** zu überführen, in der er unterstützt und vertrauenswürdig ist. Dies beinhaltet die Code-Promotion (Export der Bot-Lösung und Import in eine kontrollierte Umgebung) und möglicherweise einen formellen Überprüfungs- oder Genehmigungsschritt. Organisatorisch bedeutet dies, Kriterien zu definieren: Was rechtfertigt eine Promotion? Wer gibt die Freigabe?
- **Unterstützung und Anleitung für Maker:** Nicht alle Maker sind erfahrene Entwickler. Sie benötigen möglicherweise Hilfe bei der Befolgung von Best Practices (Festlegen geeigneter Berechtigungen in ihrem Bot, Fehlerbehandlung, effektive Nutzung von Vorlagen). Ohne Unterstützung könnten ihre Bots unsicher oder ineffizient sein. Aber IT-Teams fehlt oft die Bandbreite, um Hunderte von Citizen-Entwicklern einzeln zu unterstützen. Ein strukturiertes Programm (Champions, Vorlagen, Sprechstunden) ist erforderlich, was eine Herausforderung bei der Etablierung sein kann.

Werkzeuge & Methoden:

Die Veranstaltung stellte konkrete Werkzeuge vor, um einen strukturierten Agenten-Lebenszyklus zu implementieren und gleichzeitig die Maker zu befähigen. So können Entscheidungsträger ihre Organisation für den Erfolg aufstellen:

- **Umgebungsstrategie (Grün/Gelb/Rot-Zonen):** In Anlehnung an ein Konzept aus Governance-Modellen (und tatsächlich aus Gartners Rat, wie erwähnt), kann die IT separate **Power Platform-Umgebungen** für verschiedene Phasen der Bot-Entwicklung erstellen:
    - **„Grüne Zone" – Persönliche Entwicklungsumgebungen:** Jeder Maker erhält eine persönliche Entwicklungsumgebung (wie einen persönlichen Arbeitsbereich), um frei zu experimentieren. Diese Umgebungen haben strenge Grenzen – z. B. können sie Bots nicht mit anderen teilen (nur der Maker kann ihn verwenden), und Konnektoren zu sensiblen Systemen können eingeschränkt sein. Dieser Sandbox-Ansatz wurde in der Demo gezeigt: Jeder Benutzer wurde automatisch einer Entwickler-Umgebungsgruppe mit geltenden Richtlinien zugewiesen. Maker können ohne Risiko für andere experimentieren.
    - **„Gelbe Zone" – Team- oder Abteilungs-Testumgebungen:** Wenn ein Bot vielversprechend ist (sagen wir, ein Vertriebsteam findet einen Bot nützlich und möchte, dass einige Kollegen ihn ausprobieren), kann er in eine etwas offenere Umgebung verschoben werden. In dieser Umgebung ist das Teilen innerhalb einer definierten Gruppe (Abteilung) aktiviert, und vielleicht sind mehr Konnektoren erlaubt (da es sich jetzt um eine Teamlösung handelt, nicht nur um eine persönliche). Er ist jedoch immer noch als „Test" oder „Pilot" gekennzeichnet – mit Warnungen, dass er nicht offiziell unterstützt wird und die Nutzung sorgfältig überwacht werden sollte.
    - **„Rote Zone" – Produktionsumgebung:** Dies ist eine kontrollierte Umgebung, in der nur genehmigte, vollständig geprüfte Agenten leben. Bots hier haben typischerweise eine Überprüfung durchlaufen (Sicherheitscheck, Leistungstest, Validierung der Genauigkeit durch Fachexperten). In der Produktion kann der Bot breit zugänglich sein (sogar tenant-weit), und die IT behandelt ihn wie eine Unternehmensanwendung – mit Überwachung, SLAs (Service-Level-Agreements) bei Bedarf und Einbeziehung in Notfallwiederherstellungspläne.
    - **Unterstützende Methode:** Verwenden Sie **Umgebungsgruppen und Routing-Regeln** (Funktionen im Power Platform Admin Center), um dies zu automatisieren. Zum Beispiel wird jeder neue Entwickler (Maker) automatisch der Umgebungsgruppe „Dev Agents" (Grün) hinzugefügt. Eine Pipeline wird eingerichtet, die es einem Maker ermöglicht, seinen

Bot zur Promotion einzureichen – was einen Genehmigungsworkflow auslöst, um ihn in Test oder Prod zu verschieben.

- **Erweiterte Maker-Richtlinien:** Innerhalb dieser Entwicklungsumgebungen können Administratoren Leitplanken mit **Datenrichtlinien** (wie zuvor besprochen) und **Freigabebeschränkungen** festlegen. Zum Beispiel kann der Admin das externe Teilen von Bots aus Entwicklungsumgebungen deaktivieren (damit ein Maker seinen Entwicklungs-Bot nicht versehentlich externen Mitarbeitern oder Kunden zugänglich macht). Eine weitere leistungsstarke Funktion ist die Liste der „**eingeschränkten Aktionen**“ in Konnektoren: z. B. in der Entwicklung einem Maker-Bot erlauben, SharePoint-Daten zu lesen, aber nicht zu löschen oder externe E-Mails zu senden. Diese feingranularen Kontrollen ermöglichen es Makern, funktionale Prototypen zu erstellen und gleichzeitig potenziellen Schaden einzudämmen.
- **Inventar und Überwachung aller Agenten:** Das Admin Center enthält jetzt ein **Inventar** aller Co-Pilot-Agenten über alle Umgebungen hinweg, mit Details wie Besitzer, Umgebung, letztes Änderungsdatum, Freigabestatus usw. (Wir sahen einen Einblick davon in Zohars Demo.) Die IT sollte jemanden benennen (z. B. einen Power Platform-Admin oder einen Leiter des Center of Excellence), der dieses Inventar regelmäßig überprüft. Sie könnten beispielsweise doppelte Bots entdecken („Wir haben 3 verschiedene Spesenabrechnungs-Bots – lasst uns konsolidieren“) oder veraltete Bots („Dieser Einstellungs-FAQ-Bot wurde seit 60 Tagen nicht mehr verwendet – sollten wir ihn außer Betrieb nehmen?“).
- **Lösungen und ALM-Pipelines:** Jeder in Copilot Studio erstellte Agent ist im Hintergrund als **Power Platform-Lösung** verpackt. Das bedeutet, dass traditionelle Application Lifecycle Management (ALM)-Tools anwendbar sind. Maker (mit Anleitung) können ihre Lösung aus der Entwicklung exportieren und in Test/Prod importieren. Besser noch, die IT kann eine **automatisierte Pipeline** (vielleicht mit Azure DevOps oder GitHub über die Power Platform Build Tools) einrichten, um Lösungen nach Genehmigung zwischen Umgebungen zu befördern. Die Sitzung beschrieb eine einfach zu bedienende Pipeline-Benutzeroberfläche, bei der ein Maker auf „Bereitstellen“ drückt und nach Genehmigung der Bot in die Produktion verschoben wird. Die Schlüsselmethode für Entscheidungsträger besteht darin, einmal in die Einrichtung dieser Pipeline zu investieren, damit jede nachfolgende Promotion konsistent ist und keinen Neuerfindungsprozess erfordert.
- **CoE (Center of Excellence) Starter Kit:** Microsoft stellt ein Bündel von Werkzeugen und Best Practices (das Power Platform CoE Starter Kit) zur Verfügung, das jetzt Copilot-Governance-Komponenten enthält. Dieses Kit kann Metriken wie die Anzahl der Bots pro Umgebung verfolgen, Top-Maker identifizieren usw. Die Einführung dieser Werkzeuge gibt Entscheidungsträgern

vorgefertigte Einblicke in die Verwaltung des Maker-Ökosystems (z. B. erkennen, ob eine Umgebung ihre Kapazitätsgrenze erreicht oder ob eine bestimmte Abteilung mehr Unterstützung basierend auf den Bot-Nutzungsmustern benötigt).

- **Maker-Befähigung & Unterstützung:** Weiche Werkzeuge sind genauso wichtig wie technische. Fördern Sie eine **Champions-Community für Power Platform/Copilot-Maker**. Sie werden sich gegenseitig helfen, indem sie Lösungen, Komponenten oder gewonnene Erkenntnisse teilen (zum Beispiel könnte ein Champion eine wiederverwendbare „HR Q&A Bot-Vorlage“ veröffentlichen, die andere kopieren können, anstatt sie von Grund auf neu zu erstellen). Stellen Sie auch Kanäle für Q&A bereit – vielleicht eine monatliche „KI-Maker-Klinik“ (Live-Sitzung oder Team-Kanal, in dem IT-Experten Fragen beantworten). Dies verringert die Wahrscheinlichkeit, dass ein Maker stecken bleibt und einen nützlichen Bot aufgibt.

Durch die Etablierung dieses klaren Lebenszyklus – von der Konzeption in einer sicheren Sandbox über die schrittweise Erweiterung des Publikums bis hin zur vollständig unterstützten Produktionsbereitstellung – kann die Organisation die Kreativität ihrer Mitarbeiter nutzen, ohne die Kontrolle oder Qualität zu verlieren. Eine gute Analogie, die in der Sitzung geteilt wurde, war die Behandlung dieser KI-Agenten wie jede andere Produktentwicklung: Sie haben eine Entwicklungsphase, eine UAT-Phase (User Acceptance Testing) und eine Freigabephase, mit **Qualitätstoren** dazwischen.

Best Practices:

- **Promotionskriterien frühzeitig definieren:** Entscheiden Sie, welche Kriterien ein Bot erfüllen muss, um von der Entwicklung in den Test und dann in die Produktion zu gelangen. Zum Beispiel: „Um in die Produktion befördert zu werden, muss ein Agent Folgendes haben: mindestens eine VP-Sponsor-Freigabe, eine bestandene Sicherheitsüberprüfung der Konnektoren/Berechtigungen, ein Schulungsdokument für Endbenutzer und den Nachweis aus der Pilotnutzung, dass er genau ist (z. B. 90 % Erfolg bei der Beantwortung der Fragen der Pilotgruppe).“ Dokumentieren Sie diese, damit die Maker das Ziel kennen.
- **Namenskonventionen verwenden:** Um Umgebungen und Agenten in jeder Phase leicht zu identifizieren, verwenden Sie ein Namensschema. Z. B. Präfix für Entwicklungs-Agentennamen mit „(DEV)“ oder Umgebungsnamen klar beschriften wie „CoPilot-Dev-DeptX“. Dies wird in Admin-Listen angezeigt und vermeidet Verwirrung.

- **Kosten und Ressourcennutzung überwachen:** Wenn ein Agent Backend-Dienste aufruft (wie das Abrufen von Daten aus einem SAP-System über eine API), überwachen Sie diese API-Aufrufe. Ein schlecht gestalteter Bot könnte ein System mit zu vielen Anfragen überlasten. Die Verwaltungstools können zeigen, wie viele „Aktionen“ Bots ausführen. Setzen Sie Schwellenwerte und warnen Sie bei Anomalien (wenn ein Bot plötzlich in der Nutzung ansteigt, prüfen Sie, ob er viral geht oder schlecht funktioniert).
- **Rücksichtslos außer Betrieb nehmen:** Nicht jeder Bot wird ein Hit sein. Es ist besser, redundante/ungenutzte Agenten zu entfernen oder zusammenzuführen, um Unordnung zu reduzieren. Haben Sie eine Richtlinie (z. B. „wenn keine Nutzung in 90 Tagen, geht der Agent in Quarantäne; wenn keine in 180 Tagen, wird er unveröffentlicht“). Maker sollten darüber informiert werden, dass ihre Lösung, wenn sie keine Traktion gewinnt, auslaufen könnte – und das ist in Ordnung, konzentrieren Sie sich auf Projekte mit höherem Wert.
- **Erfolge erkennen und skalieren:** Umgekehrt, wenn ein bestimmter Agent viel Zeit spart oder eine hohe Akzeptanz findet, heben Sie ihn hervor. Formalisieren Sie ihn möglicherweise – z. B. wird der erfolgreiche Sales-Bot, der von einem Vertriebsmanager erstellt wurde, jetzt zu einer von der IT unterstützten Anwendung in der Produktion, um sicherzustellen, dass er die Ressourcen und den Support hat, die er benötigt, wenn er geschäftskritisch wird. Belohnen Sie den Maker (könnte so einfach wie eine Anerkennung durch die Führung sein), um andere zu motivieren.

Durch strukturiertes Lebenszyklusmanagement können Unternehmen einen **lebendigen internen Marktplatz für KI-Lösungen** genießen, der sich von Basisideen zu offiziell sanktionierten Werkzeugen entwickelt. Dies fördert eine Innovationskultur – Mitarbeiter fühlen sich befähigt, Probleme zu lösen – und doch behält die Organisation die Kontrolle über die gesamte KI-Landschaft, mit Sichtbarkeit und Governance bei jedem Schritt. Entscheidungsträger werden im Wesentlichen zu **Kuratoren der Innovation**, die die Ideen, die funktionieren, hochskalieren und diejenigen, die nicht funktionieren, anmutig herunterskalieren, während alles sicher und konform bleibt.

7. Sichere Befähigung von Makern – Zonen, Umgebungen und Self-Service-Entwicklung

(Dieser Abschnitt ergänzt den vorherigen, indem er auf den Aspekt der „Befähigung von Makern“ eingeht und praktische Anleitungen gibt, wie Mitarbeiter in die Lage versetzt werden können, Copilot-Agenten auf sichere und kontrollierte Weise zu erstellen.)

Einer der einzigartigen Vorteile der Power Platform und von Copilot Studio ist, dass sie „Citizen Developers“ – Geschäftsanwendern mit Fachexpertise – ermöglichen, ihre eigenen Mini-Copilots (Bots) ohne aufwändige Programmierung zu erstellen. Sitzung 7 konzentrierte sich darauf, wie man **diese Maker mit den Werkzeugen und dem Zugang ausstattet, die sie benötigen, während die Governance aufrechterhalten wird**. Im Wesentlichen: Wie kultiviert man eine **Innovations-Sandbox** im gesamten Unternehmen.

Bedeutung für Entscheidungsträger:

Aus Sicht der Führungsebene kann die Förderung von Innovation und Automatisierung auf Basisebene die Kapazität der IT zur Bereitstellung von Lösungen erheblich erweitern. Geschäftsteams haben oft Nischenbedürfnisse, die die zentrale IT möglicherweise nicht schnell erfüllen kann; wenn diese Teams sicher ihre eigenen KI-Assistenten erstellen können, wird das gesamte Unternehmen agiler. Dies muss jedoch strukturiert angegangen werden, um Chaos zu vermeiden. Durch die sichere Befähigung von Makern erreichen Entscheidungsträger:

- **Schnellere Problemlösung:** Die Personen, die mit einem Problem konfrontiert sind (z. B. Kundendienstmitarbeiter), können ein KI-Werkzeug erstellen, um ihnen zu helfen (z. B. ein Bot, der Antworten aus internen Wissensdatenbanken vorschlägt), ohne in einer langen IT-Warteschlange zu warten.
- **Höhere Akzeptanz:** Menschen sind natürlich mehr in Werkzeuge investiert, die sie erstellen oder anpassen. Eine Verkäuferin wird eher einen Verkaufsunterstützungs-Copilot verwenden, den ihr Team erstellt und auf ihre Sprache und ihren Prozess zugeschnitten hat. Dieser Bottom-up-Ansatz kann die Akzeptanz besser vorantreiben als Top-down-Mandate.
- **Verteilte Innovation mit zentraler Aufsicht:** Über das Zonenmodell arbeiten Maker in kontrollierten Umgebungen. Die Führung behält die Aufsicht (durch Inventar- und Genehmigungsprozesse, wie besprochen) – und erhält so „das Beste aus beiden Welten“ (Kreativität und Kontrolle).
- **Aufbau einer digitalen Kultur:** Die Befähigung von Mitarbeitern, Lösungen zu erstellen, fördert eine Kultur des Lernens und der Innovation. Es sendet eine

Botschaft, dass die Organisation den Ideen ihrer Mitarbeiter vertraut und in sie investiert (was die Mitarbeiterbindung und das Engagement fördern kann).

Herausforderungen:

Die Befähigung von Makern ist nicht ohne Tücken, typischerweise im Zusammenhang mit der Sicherstellung der Qualität, der Vermeidung von Redundanz und der Bereitstellung ausreichender Unterstützung:

- **Kompetenzlücken:** Nicht alle Mitarbeiter haben den Hintergrund, um effektive Prompts oder logische Abläufe zu entwerfen. Einige könnten suboptimale Agenten erstellen (z. B. ein Bot, der aufgrund schlechter Prompts falsch antwortet). Wenn viele minderwertige Bots im Umlauf sind, könnte dies die Einstellung gegenüber der Technologie beeinträchtigen. Schulungen und Vorlagen wurden als Lösungen hierfür diskutiert.
- **Umfang der Unterstützung:** Wenn Sie, sagen wir, 500 Maker befähigen, wie unterstützen Sie sie? Sie werden Fragen haben wie „Wie verbinde ich mich mit System X?“ oder „Warum antwortet mein Bot nicht richtig?“. Traditionelle Helpdesks sind möglicherweise noch nicht darauf vorbereitet, von Bürgern entwickelte KI zu unterstützen.
- **Governance-Müdigkeit:** Das richtige Gleichgewicht zu finden ist schwierig; wenn sich Maker durch IT-Regeln zu sehr eingeschränkt fühlen (z. B. dürfen sie in der Entwicklung keine benötigte Datenquelle verwenden), könnten sie frustriert werden oder versuchen, Prozesse zu umgehen. Umgekehrt, wenn sich die IT von der Menge neuer Lösungen überfordert fühlt, könnten sie versucht sein, zu stark einzuschränken und die Bemühungen zur Befähigung zunichtezumachen. Ein kontinuierlicher Dialog (ein Center of Excellence, das IT und Maker überbrückt) ist erforderlich.
- **Integration und Wiederverwendung:** Ohne Koordination könnten Maker Anstrengungen duplizieren. Z. B. erstellen zehn HR-Mitarbeiter jeweils einen PTO-Genehmigungs-Bot für ihre Region – vielleicht leicht unterschiedlich. Es gibt eine verpasste Gelegenheit, Komponenten zu teilen oder zu einer Lösung zu konvergieren, die mehrere Regionen abdeckt. Maker dazu zu bringen, ihre Arbeit zu teilen und bestehende Assets wiederzuverwenden (anstatt neu zu bauen), ist eine kulturelle und technische Herausforderung. (Die Veranstaltung sprach über Champion-Communities und Vorlagen, um dies anzugehen.)
- **Kostenmanagement:** Wenn jede Abteilung beginnt, mehrere KI-Agenten zu betreiben, die verschiedene APIs oder Dienste aufrufen, können die Kosten steigen. Es ist entscheidend, den Verbrauch zu überwachen, wie in Sitzung 8 behandelt, und möglicherweise die Nutzung an die Abteilungen zurückzuverrechnen, um effiziente Designs zu fördern.

Werkzeuge & Methoden:

Um Maker innerhalb sicherer Grenzen zu befähigen, kann die Organisation mehrere Strategien umsetzen und Werkzeuge nutzen:

- **Gestufte „Zonen“ mit Self-Service-Provisionierung:** Wie bereits beschrieben, richten Sie **Grüne Zone (Persönliche Entwicklung)**-Umgebungen ein, die automatisch für jeden Benutzer erstellt werden, der bauen möchte. Dies kann per Richtlinie automatisiert werden – zum Beispiel, wenn jemand zum ersten Mal Copilot Studio öffnet, wird eine Umgebung für ihn mit voreingestellter Governance provisioniert. Der Admin kann dies über **Power Platform Environment Templates** und die Routing-Regel („Entwickler erstellt Umgebung beim ersten Ausführen“) tun. Dies senkt die Reibung – kein langwieriger Anforderungsprozess, um mit dem Bauen zu beginnen – und platziert den Maker dennoch in einem gesteuerten Raum.
- **Vorgefertigte Vorlagen und Komponenten:** Stellen Sie Makern **Vorlagen** für gängige Agententypen zur Verfügung (die Sitzung erwähnte Microsofts interne Bibliothek von Anwendungsfallvorlagen). Zum Beispiel könnte eine „FAQ Bot“-Vorlage bereits einen grundlegenden Frage-Antwort-Fluss und Verbindungen zu gängigen Datenquellen enthalten; der Maker fügt nur seinen spezifischen Q&A-Inhalt ein. Vorlagen gewährleisten eine Grundqualität und Sicherheit (da die IT Best Practices darin einbetten kann) und beschleunigen die Entwicklung. Pflegen Sie ebenfalls eine **Komponentenbibliothek** (über die Lösungsbibliothek der Power Platform oder GitHub), in der Maker Teile finden und wiederverwenden können (wie eine „Ergebnis per E-Mail senden“-Komponente oder einen vorgefertigten Konnektor zum CRM).
- **Maker-Schulungsprogramm:** Starten Sie eine mundgerechte Schulungsreihe für neue KI-Maker. Dies könnte umfassen:
    - Einen **initialen Workshop** (oder ein aufgezeichnetes Video) zu „Wie man seinen ersten Copilot-Agenten baut“, der die Grundlagen abdeckt und die Erstellung eines einfachen Bots in 30 Minuten demonstriert.
    - **Sprechstunden:** Ein wöchentlicher offener Anruf, bei dem Maker Fragen stellen oder Probleme mit Unterstützung von Experten-IT oder Champion-Benutzern beheben können.
    - **Interne Community-Foren:** Nutzen Sie einen Teams-Kanal oder eine Yammer (Viva Engage)-Community, die den Power Platform/Copilot-Makern gewidmet ist. Fördern Sie dort Q&A und gegenseitige Hilfe. Wie in Carolinas Sitzung erwähnt, kommt die beste Unterstützung oft von Gleichgesinnten. Dies fördert auch die Anerkennung (Leute teilen ihre Erfolge und inspirieren andere).

    - **Champions & Mentoren:** Identifizieren Sie frühe Power-Maker und erkennen Sie sie offiziell als **Champions** an. Diese Personen könnten die Community moderieren oder Schulungen in lokalen Abteilungen durchführen. Richten Sie vielleicht einen Champion pro Abteilung ein, der die erste Anlaufstelle für Kollegen ist, die versuchen, etwas zu bauen.
- **Klarer Einreichungs- & Genehmigungsworkflow:** Stellen Sie einen einfachen Mechanismus bereit (wahrscheinlich in Copilot Studio integriert oder über einen Power Automate-Flow), damit ein Maker sagen kann: „Ich denke, mein Bot ist bereit, mit dem Team geteilt zu werden“ oder „bereit für den unternehmensweiten Einsatz“. Die Demo der Sitzung zeigte einen „Bereitstellen“-Button, der eine Genehmigungsanfrage auslöst. Dahinter kann sich ein Power Automate-Genehmigungsflow an eine bestimmte Genehmigergruppe (vielleicht das Center of Excellence oder das IT-Governance-Board) verbergen. Wenn der Genehmiger ablehnt, fügen Sie Feedback hinzu („Bitte fügen Sie eine Nutzungsanleitung hinzu und beheben Sie diese 2 Sicherheitsbefunde, dann erneut einreichen“). Wenn genehmigt, veröffentlicht die Pipeline es in einer Zielumgebung. Diese Methode stellt sicher, dass kein Self-Service-Bot ohne Aufsicht eine breite Verbreitung findet, rationalisiert aber auch die Promotion (ein Ein-Klick für den Maker).
- **Nutzungsüberwachung & Maker-Anerkennung:** Behalten Sie im Auge, welche von Makern erstellten Agenten an Zugkraft gewinnen. Nutzen Sie die Analysen, um die Top-10-Community-erstellten Bots nach Nutzung zu finden. Tun Sie dann zwei Dinge: (1) Erwägen Sie ihre Promotion zum offiziellen IT-Support (damit sie robustes Hosting, vielleicht etwas Entwickler-Feinschliff und formale SLAs bei Bedarf erhalten). (2) Veröffentlichen Sie sie als Erfolgsgeschichten („Der Social-Media-Copilot des Marketingteams – gebaut von Jane Doe – wird jetzt 500 Mal pro Woche verwendet und hat die Antwortzeit auf Twitter um 50 % verkürzt“). Diese Anerkennung belohnt nicht nur den Maker, sondern ermutigt auch andere, zu sehen, was möglich ist, und nachzuziehen.
- **Kostentransparenz:** Wenn Sie Pay-as-you-go (PAYG)-Abrechnung für Umgebungen aktivieren (wie von Ameya in Sitzung 8 beschrieben), stellen Sie sicher, dass die Abteilung jedes Makers über die Kosten informiert ist, die ihre Bots verursachen (durch Rückverrechnung oder zumindest ein Dashboard). Dies neigt dazu, Maker umsichtiger zu machen – z. B. werden sie unnötige Komplexität vermeiden, die API-Aufrufe in die Höhe treibt – und es verhindert Überraschungen für das Management. Wenn ein Agent extrem nützlich, aber kostspielig ist, können Entscheidungsträger wissentlich entscheiden, diese Nutzung zu finanzieren (oder zu optimieren).

Best Practices:

- **Umgebungsdisziplin wahren:** Lassen Sie nicht zu, dass eine Umgebung zu einer Müllhalde für zu viele Projekte wird. Ermutigen Sie Maker, in ihrer persönlichen Umgebung oder einer dedizierten Teamumgebung zu arbeiten. Dies vermeidet Überschneidungen und Verwirrung darüber, wem welcher Bot gehört. Das Umgebungs-Routing und die Gruppeneinrichtung automatisieren viel davon, aber überwachen Sie, ob Leute anfangen, Ad-hoc-Umgebungen zu erstellen, und bringen Sie sie gegebenenfalls unter die Fittiche des CoE.
- **Quellcodeverwaltung für komplexe Bots durchsetzen:** Wenn der Bot einer bestimmten Abteilung komplex wird (mehrere Maker arbeiten zusammen, viele Komponenten), führen Sie sie in die Verwendung von Quellcodeverwaltung (wie das Einchecken von Lösungsdateien in ein Git-Repo) und Versionierung ein. Obwohl dies für reine Geschäftsanwender vielleicht fortgeschritten ist, kann ein versierter Champion oder ein IT-Entwickler helfen. Dies stellt sicher, dass, wenn mehrere Personen einen Agenten verbessern, sie sich nicht gegenseitig die Arbeit überschreiben und es eine Rollback-Fähigkeit gibt, wenn ein Update etwas kaputt macht. Die Power Platform unterstützt den Export von Lösungen als Code für diesen Zweck.
- **Periodische Maker-Showcases:** Über die reine Unterstützung hinaus, feiern Sie Innovation. Veranstalten Sie vierteljährlich eine „Copilot Agent Expo“ (virtuelles Meeting oder internes Event), bei der Maker die von ihnen gebauten Agenten vorführen, insbesondere solche, die ein echtes Problem gelöst haben. Entscheidungsträger und Kollegen können teilnehmen, Fragen stellen und überlegen, diese Ideen auf andere Einheiten zu übertragen. Dies schafft Begeisterung und einen gesunden Wettbewerbsgeist („Wenn die Personalabteilung einen großartigen Onboarding-Bot gebaut hat, können wir in der Finanzabteilung einen großartigen Spesen-Bot bauen“). Es hilft auch, doppelte Anstrengungen aufzudecken – zwei Gruppen könnten erkennen, dass sie sich für eine einzige Lösung zusammenschließen können.
- **Governance nach Bedarf aktualisieren:** Lernen Sie davon, wie Maker die Plattform tatsächlich nutzen. Vielleicht haben Sie ursprünglich einen bestimmten Konnektor blockiert (weil Sie dachten, er sei riskant), stellen aber später fest, dass er benötigt wird und das Risiko gemanagt werden kann – dann entsperren Sie ihn. Oder umgekehrt, Sie haben etwas erlaubt und dann Missbrauch gesehen – also verschärfen Sie es. Governance-Richtlinien (wie Datenverlustregeln oder Umgebungseinschränkungen) sollten regelmäßig im Lichte des Maker-Feedbacks und der Sicherheitsüberwachungsergebnisse überprüft werden. Binden Sie Maker in diese Überprüfung ein; sie könnten vorschlagen: „Wenn Sie Konnektor X erlauben würden, könnten wir Y tun – aber wie wäre es, wenn wir ihn aktivieren und zustimmen, ihn nur in der Entwicklung

zu verwenden, nicht in der Produktion?“ Dieser kollaborative Ansatz verfeinert die Befähigung mit Verantwortung.

Im Wesentlichen bedeutet **sichere Befähigung von Makern**, ein Rahmenwerk zu schaffen, das **standardmäßig freizügig und präventiv im Design** ist. Es schafft eine **Sandbox mit Mauern**: innen blüht die Kreativität; die Mauern verhindern, dass sie aus den Fugen gerät. Durch klare Zonen, unterstützende Gemeinschaften und intelligente Aufsicht können Entscheidungsträger Hunderte von Mitarbeitern zu Mitgestaltern von KI-Lösungen machen und so die Fähigkeit der Organisation vervielfachen, die Copilot-Technologie in jeder Nische des Unternehmens zu nutzen. Dies beschleunigt nicht nur die digitale Transformation, sondern schafft auch ein Gefühl der Eigenverantwortung und eine Innovationskultur auf allen Ebenen.

8. Erstellung sicherer unternehmensweiter Agenten – Best Practices und Compliance-Kontrollen

Wenn Maker und IT-Profis zusammenarbeiten, um vielversprechende Copilot-Agenten in die Produktion zu überführen (die „Rote Zone“ unseres Governance-Modells), wird es entscheidend sicherzustellen, dass diese unternehmensweiten Agenten **sicher, konform und zuverlässig** sind. Sitzung 8 befasste sich mit den Details der Absicherung von Copilot-Agenten, die zu einem Kernbestandteil von Geschäftsprozessen geworden sind. Es wurde behandelt, wie man Sicherheit in den Entwicklungsprozess einbaut, Anmeldeinformationen und APIs sicher verwaltet und die Einhaltung von Vorschriften bei der Nutzung von KI aufrechterhält. Im Wesentlichen geht es darum, einen von Bürgern entwickelten Bot zu einer **anwendungsreifen Unternehmensanwendung** zu professionalisieren.

Bedeutung für Entscheidungsträger:

Wenn ein KI-Agent den unternehmensweiten Maßstab erreicht (z. B. wird ein „Spesenabrechnungs-Copilot“ jetzt unternehmensweit zur Unterstützung bei Spesenabrechnungen verwendet), unterliegt er den gleichen Erwartungen wie jedes andere wichtige System. Entscheidungsträger müssen sicherstellen, dass er:

- **Daten schützt:** Der Agent berührt wahrscheinlich sensible Daten (Finanzunterlagen, persönliche Informationen, Strategiedokumente). Er muss alle Sicherheitsstandards (Verschlüsselung, ordnungsgemäße Zugriffskontrolle) einhalten und darf keine neuen Schwachstellen einführen.
- **Gesetze einhält:** Wenn der Agent personenbezogene Daten verarbeitet, tut er dies im Einklang mit der DSGVO? Wenn er Inhalte vorschlägt, ist er zugänglich (für Arbeitnehmer mit Behinderungen) und unvoreingenommen? Führungskräfte müssen diese Fragen zuversichtlich beantworten können.
- **Zuverlässig funktioniert:** Ausfallzeiten oder Fehler bei einem weit verbreiteten Agenten können die Arbeit stören. Die Planung für hohe Verfügbarkeit, Lastkapazität und klare Zuständigkeiten für den Support (wer repariert den Bot, wenn er kaputt geht?) wird notwendig.
- **IT-Standards entspricht:** Er sollte dokumentiert, versioniert, in der Produktion überwacht und in Notfallwiederherstellungspläne einbezogen werden. Wenn sich hinter dem Bot ein Azure-Dienst oder eine Datenbank befindet, sollte dieser Dienst im Inventar der IT und unter Beobachtung stehen.

Die Quintessenz: Ein unternehmensweiter Copilot-Agent sollte mit der gleichen Strenge behandelt werden wie jede offizielle Softwareanwendung, die das Unternehmen zum

Betrieb verwendet. Entscheidungsträger können kritische Bots nicht im „Hobby“-Status belassen; sie müssen sie **industrialisieren**.

Herausforderungen:

Die Erstellung sicherer, konformer KI-Agenten birgt besondere Herausforderungen, wie zum Beispiel:

- **Sichere Integration von Datenquellen:** Unternehmens-Bots verbinden sich oft mit zahlreichen Systemen (CRM, ERP, HR-Systeme). Die Verwaltung der **Anmeldeinformationen** (API-Schlüssel, Verbindungszeichenfolgen) für diese innerhalb des Bots ist sensibel. Das Hartcodieren eines Passworts ist offensichtlich schlecht – aber selbst das Speichern von Anmeldeinformationen im Klartext in einer Power Platform-Umgebung wird nicht empfohlen. Die Verwendung eines **Key Vault** oder eines anderen Geheimnisspeichers ist die beste Praxis, aber Maker sind damit möglicherweise nicht vertraut.
- **Mandantenfähigkeit und Geltungsbereich:** Einige Agenten müssen möglicherweise mehrere Abteilungen bedienen, aber mit Datenpartitionierung (die Daten jeder Abteilung bleiben privat). Sicherzustellen, dass der Agent Inhalte korrekt nach Benutzerrolle filtert, ist eine Herausforderung. Es könnte erforderlich sein, eine „**Datensegmentierungs**“-Logik zu implementieren. Wenn schlecht konzipiert, könnte es Daten über Gruppen hinweg lecken (ein Sicherheitsfehler).
- **Verhalten von KI-Modellen:** Große Sprachmodelle (LLMs) erzeugen gelegentlich unerwartete oder unerwünschte Ausgaben (mögliches Compliance-Problem, wenn es beispielsweise eine unsensible Phrase generiert oder versehentlich voreingenommene Sprache aus Trainingsdaten verwendet). Die Gewährleistung von **ethischem KI-Verhalten** im Unternehmensmaßstab ist schwierig – es erfordert ständige Überwachung und Feinabstimmung (z. B. das Hinzufügen bestimmter Begriffe zu einer Sperrliste, die Verwendung der Inhaltsfilter von OpenAI oder das Anpassen der Prompts, die der Agent verwendet, um den Ton zu steuern).
- **Change Management für KI-Verhalten:** Traditionelle Software tut, was sie programmiert wurde, was vorhersehbar ist. KI-Agenten können sich subtil ändern, wenn das Modell aktualisiert wird oder sie aus neuen Daten lernen (bei kontinuierlichem Lernen). Dies kann Benutzer verwirren („Früher hat es anders geantwortet“). Die Verwaltung der **Evolution des KI-Verhaltens** – Änderungen kommunizieren, bei Bedarf neu schulen – ist eine neue Art der Wartung für die IT.
- **Regulatorische Compliance:** Wenn das Unternehmen in einer regulierten Branche tätig ist (Finanzen, Gesundheitswesen, Regierung), muss jede neue Technologie Audits bestehen. Auditoren könnten jetzt fragen: „Zeigen Sie mir die

Trainingsdaten dieser KI“ oder „Wie verhindern Sie, dass sie Kundennummern preisgibt?“. Dokumentation und Nachweise für Auditoren (die möglicherweise nicht KI-versiert sind) sind eine Herausforderung. Die Sitzung erwähnte wahrscheinlich die Nutzung der **Compliance-Angebote von Azure OpenAI** oder die Führung von Protokollen der KI-Interaktionen für Audit-Trails.

Werkzeuge & Methoden:

Um diese Herausforderungen anzugehen, wurden mehrere Best Practices und Werkzeuge hervorgehoben:

- **Sicheres Verbindungsmanagement:** Verwenden Sie den **Azure Key Vault-Konnektor der Power Platform** oder umgebungsbezogene sichere Einstellungen, um Anmeldeinformationen zu speichern, die Bots zur Verbindung mit externen Systemen verwenden. Auf diese Weise sehen Maker niemals Passwörter im Klartext und das Rotieren von Schlüsseln ist einfacher (im Vault aktualisieren, der Bot holt sich den neuen Schlüssel). Wenden Sie zusätzlich das Prinzip des **geringsten Privilegs** an: Wenn der Bot nur Lesezugriff auf eine Datenbank benötigt, geben Sie ihm keine Schreibberechtigungen. Dies begrenzt den Schaden bei Missbrauch.
- **Datentrennung durch Zugriffskontrolle:** Wenn ein Unternehmens-Bot mehrere Gruppen bedient, implementieren Sie Datenzugriffskontrollen in seiner Logik. Zum Beispiel könnte ein Bot, der HR-Richtlinienfragen für alle Mitarbeiter beantwortet, Daten von einer SharePoint-Website abrufen, die jeder lesen kann – das ist in Ordnung. Aber ein „Sales Deal Insight“-Bot, der Verkaufsdaten bereitstellt, sollte die Antworten auf die Daten beschränken, auf die der abfragende Benutzer Rechte hat. Dies kann durch die Verwendung der **Identität des Benutzers (Token)** erfolgen, wenn der Bot die Datenbank abfragt, nicht eines generischen Dienstkontos. Die Plattform unterstützt die Verwendung des **Kontexts des aktuellen Benutzers** in Konnektoren (in einigen Systemen als „Benutzerdelegation“ bezeichnet). Sicherzustellen, dass der Bot dies verwendet, verhindert Datenlecks über verschiedene Datenbereiche hinweg. Das Testen dieses Szenarios ist eine empfohlene Methode: Lassen Sie einen Benutzer aus Abteilung A den Bot nach den Daten von Abteilung B fragen – bestätigen Sie, dass er ablehnt oder keine Daten findet.
- **Rigorose Tests & Validierung:** Bevor ein Bot für die Produktion „gesegnet“ wird, führen Sie **Penetrationstests** ähnlich wie bei einer Web-App durch. Versuchen Sie Prompt-Injektionen, versuchen Sie, unbefugte Informationen abzurufen, füttern Sie ihn mit kniffligen Eingaben. Bewerten Sie seine Worst-Case-Ausgaben. Dies kann von internen Sicherheitsteams oder sogar externen Spezialisten durchgeführt werden. Die Sitzung erwähnte wahrscheinlich eine KI-

Sicherheitscheckliste (z. B. Test mit absichtlich fehlerhaften Abfragen, um zu sehen, ob sensible Inhalte durchrutschen). Erst wenn er diese Tests besteht, sollte er zur breiten Nutzung übergehen.

- **Kontinuierliche Überwachung in der Produktion:** Auch nach der Bereitstellung richten Sie **Warnungen oder Protokolle für Anomalien** ein. Verwenden Sie beispielsweise **Azure Application Insights**, wenn der Bot auf Azure gehostet wird, um Fehler oder ungewöhnliche Aktivitätsvolumina zu verfolgen. **Purview Communication Compliance** kann laufende Interaktionen auf Richtlinienverstöße überwachen (wie für Insider-Risiken besprochen). Machen Sie jemanden dafür verantwortlich, diese Protokolle regelmäßig zu überprüfen – ähnlich wie ein Sicherheitsadministrator Firewall-Protokolle überprüft. Wenn etwas seltsam aussieht (sagen wir, ein Nutzungsanstieg um 2 Uhr morgens oder wiederholte Inhaltswarnungsauslöser), untersuchen Sie es umgehend.
- **Modell- und Prompt-Updates:** Pflegen Sie die **Prompts/Anweisungen**, die der Bot verwendet, als Code oder Konfiguration, die durch eine Änderungskontrolle geht. Wenn Sie feststellen, dass der Bot eine unangemessene Antwort gibt, müssen Sie möglicherweise den System-Prompt (die Basisanweisungen, denen er immer folgt) anpassen. Haben Sie einen Prozess dafür: Änderung vorschlagen, mit Beispielfragen testen, um zu sehen, ob es das Problem behebt und andere nicht schädigt, dann das Prompt-Update bereitstellen. Bleiben Sie außerdem bei Ihrem Modellanbieter (OpenAI usw.) über Modellverbesserungen oder -änderungen auf dem Laufenden. Manchmal kann der Wechsel zu einer neueren Modellversion die Qualität verbessern oder das Risiko schlechter Ausgaben verringern – aber testen Sie gründlich, da es sich auch anders verhalten könnte.
- **Compliance-Dokumentation:** Führen Sie einen **Bericht über das Design des Bots** für Auditzwecke: auf welche Datenquellen er zugreift, wie er gesichert ist, welche Filterung angewendet wird (z. B. verwendet er Azure OpenAI mit integrierter Inhaltsfilterung auf Schweregrad X, er protokolliert alle Prompts und Antworten für 30 Tage usw.). Wenn Sie branchenspezifische Anforderungen haben (HIPAA für Gesundheitsdaten zum Beispiel), geben Sie explizit an, wie der Bot diese erfüllt (vielleicht enthält er keine Patientenidentifikatoren in Antworten usw.). Diese Dokumentation, obwohl mühsam, wird bei einer Compliance-Überprüfung oder einem Zertifizierungsprozess viel Zeit sparen.
- **Nutzen Sie die Unternehmenseinstellungen von Microsoft:** CoPilot/OpenAI-Dienste bieten bestimmte Unternehmenseinstellungen – zum Beispiel die Möglichkeit, zu begrenzen, welche Modelle verwendet werden können (vielleicht die Verwendung von nicht genehmigten Modellendpunkten verbieten), oder den KI-Dienst in einer bestimmten Geografie für die Datenresidenz zu hosten. Stellen

Sie sicher, dass diese Einstellungen mit Ihren Unternehmensrichtlinien übereinstimmen.

Best Practices:

- **Behandeln Sie den Bot als Produkt:** Weisen Sie jedem wichtigen Unternehmens-Bot einen „**Product Owner**“ oder ein Owner-Team zu. Diese Person stellt sicher, dass das Wissen des Bots auf dem neuesten Stand ist (indem sie ihm neue FAQs oder Daten zuführt, wenn sich die Dinge ändern), überwacht Fehlerbehebungen und überwacht das Benutzerfeedback. Es ist vergleichbar mit einem Owner für eine interne Anwendung. Der Bot läuft nicht von selbst – Menschen und Prozesse halten ihn relevant und korrekt.
- **Regelmäßige Rezertifizierung:** Legen Sie einen Zeitplan fest (vielleicht jährlich oder bei größeren Änderungen), um den Bot erneut gegen Sicherheits- und Compliance-Standards zu bewerten. So wie Sie vielleicht jährlich die Benutzerzugriffsberechtigungen überprüfen, überprüfen Sie jährlich den Bot: Folgt er immer noch allen Richtlinien? Gab es in diesem Jahr eine neue Compliance-Regel, an die sich der Bot halten muss? Wenn beispielsweise ein neues Datenschutzgesetz die automatisierte Entscheidungsfindung einschränkt, stellen Sie sicher, dass die Verwendung personenbezogener Daten durch den Bot immer noch mit dem neuen Gesetz konform ist.
- **Sichern Sie das Gehirn des Bots:** Wenn der Bot auf bestimmten Wissensdatenbanken (SharePoint-Dokumente, Q&A-Paare in einer Datenbank) beruht, behandeln Sie diesen Inhalt als kritische Daten. Sichern Sie ihn genauso wie Sie Datenbanken sichern. Wenn eine SharePoint-Website, die den Bot füttert, beschädigt oder gelöscht wird, sollten Sie sie wiederherstellen können, um das „Gehirn“ des Bots nicht zu verlieren. Erwägen Sie auch einen **Fallback-Modus** für den Bot – z. B. wenn der KI-Dienst nicht erreichbar ist, leiten Sie die Benutzer vielleicht zu einer manuell kuratierten FAQ-Seite. Diese Notfallplanung ist Teil der Unternehmensreife.
- **User Acceptance Testing (UAT) mit Stakeholdern:** Bevor Sie den Bot breit freigeben, beziehen Sie eine Gruppe von Endbenutzern oder Fachexperten ein, um den Bot in realen Szenarien auszuprobieren. Ihr Feedback wird Probleme aufdecken, die automatisierte Tests möglicherweise nicht finden – z. B. „Der Ton des Bots in den Antworten fühlt sich für den Kundenservice zu kurz an; können wir ihn freundlicher gestalten?“ oder „Er hat ein entscheidendes Detail übersehen, das wir normalerweise immer einschließen.“ Integrieren Sie dieses Feedback, um Prompts oder Datenquellen zu verfeinern. Dies stellt sicher, dass der Bot den Geschäftsanforderungen wirklich entspricht und von den Benutzern akzeptiert wird.

- **Schrittweiser Rollout und Feedbackschleifen:** Auch nach bestandenen Tests sollten Sie den Unternehmens-Bot in Phasen ausrollen (zuerst an eine Abteilung, dann an alle). Überwachen Sie genau und richten Sie einfache Feedback-Kanäle ein (wie ein „War diese Antwort hilfreich?“-Daumen-hoch/runter, das Antworten protokolliert). Nutzen Sie dies zur kontinuierlichen Verbesserung. Entscheidungsträger sollten dem Team ermöglichen, den Bot regelmäßig zu iterieren, anstatt anzunehmen, dass er „einmal und fertig“ ist. Diese agile Denkweise hält den Bot effektiv, während sich Geschäftsinhalte und -bedürfnisse weiterentwickeln.

Durch die rigorose Anwendung dieser Best Practices und Kontrollen kann ein unternehmensweiter Copilot-Agent zu einem **vertrauenswürdigen digitalen Assistenten** in der Organisation werden, der so zuverlässig ist wie jede offizielle Softwareanwendung. Entscheidungsträger können diese Agenten dann wirklich fördern, da sie wissen, dass sie mit der gleichen Sorgfalt wie jedes andere Unternehmenssystem gebaut und gewartet wurden – von der Sicherheitsarchitektur bis zur Benutzerschulung. Dies erschließt das volle Potenzial der KI-Unterstützung: breite Nutzung gepaart mit starken Schutzmaßnahmen, was letztendlich zu erheblichen Effizienzsteigerungen und Innovationen im großen Maßstab führt.

9. Förderung der Akzeptanz und Best Practices – Benutzerbefähigung, Schulung und Kultur

Die beste Governance und die am besten gebauten Lösungen bedeuten wenig, wenn die Endbenutzer Copilot nicht tatsächlich in ihrer täglichen Arbeit nutzen. Sitzung 9 war der **praktischen Anleitung zur Akzeptanz von KI und Zusammenarbeit** gewidmet, im Wesentlichen der Change-Management-Seite des Copilot-Rollouts. Sie betonte Strategien, um Mitarbeitern zu helfen, Copilot anzunehmen, zu lernen, wie man ihn effektiv nutzt, und ihn in ihre Routinen zu integrieren. Für Entscheidungsträger ist dies eine Top-Priorität: Der ROI von Copilot wird nur realisiert, wenn die Leute ihn nutzen; daher ist die **Benutzerakzeptanz** kein weicher Nebengedanke – es ist ein kritischer Erfolgsfaktor, der mit der gleichen Strenge wie die technische Bereitstellung gemanagt werden muss.

Bedeutung für Entscheidungsträger:

Als Führungskräfte ist es entscheidend, eine Kultur zu fördern, in der KI-Werkzeuge akzeptiert und aktiv genutzt werden. Ohne gezielte Akzeptanzbemühungen:

- **Produktivitätsgewinne stagnieren:** Wenn, sagen wir, nur 30 % der Mitarbeiter Copilot ausprobieren und viele zu alten Arbeitsweisen zurückkehren, verpasst die Organisation potenzielle Verbesserungen bei Leistung und Effizienz.
- **Ungleiche Nutzung = Ungleiche Vorteile:** Einige Teams könnten vorpreschen (indem sie Copilot zur Automatisierung von Aufgaben nutzen), während andere zurückbleiben (alles manuell erledigen). Dies kann zu Leistungsungleichgewichten und sogar zu moralischen Problemen führen („Warum hat dieses Team leichtere Arbeitslasten? Oh, sie haben die KI verstanden und wir nicht.“).
- **Widerstand und Missverständnisse:** Neue Technologien erzeugen oft Unsicherheit oder Angst (z. B. „Wird das meinen Job übernehmen?“ oder „Ich bin nicht technikaffin genug dafür.“). Wenn die Führung diese Bedenken nicht direkt anspricht, könnten einige Mitarbeiter bewusst oder unbewusst der Nutzung von Copilot widerstehen und seinen Wert untergraben.
- **Nicht realisierter Return on Investment:** Nach der Bezahlung von Lizenzen und Entwicklung bedeutet eine geringe Akzeptanz eine schlechte Rendite. Ein konzertiertes Akzeptanzprogramm stellt sicher, dass die Investition in tatsächliche Arbeitsablaufänderungen und Ergebnisse umgesetzt wird.

Herausforderungen:

Die Förderung der Akzeptanz beinhaltet menschliche Faktoren, die unvorhersehbar sein können. Einige häufige Herausforderungen, die erwähnt wurden, waren:

- **Veränderungsaversion:** Mitarbeiter, die mit bestehenden Prozessen vertraut sind, könnten Copilot als unnötige oder einschüchternde Veränderung ansehen. Es kann einen **Lernkurveneffekt** geben, bei dem anfängliche Pannen (wie Copilot, der eine unvollkommene Antwort gibt) dazu führen, dass sie voreilig sagen: „Das ist nichts für mich."
- **Vertrauens- und Genauigkeitsbedenken:** Wenn Benutzer an der Genauigkeit der Copilot-Ausgaben zweifeln, werden sie es nicht verwenden. Jedes Mal, wenn Copilot einen Fehler macht (und das wird er gelegentlich), kann das Vertrauen beschädigt werden. Ohne dies anzusprechen (Benutzer schulen, Ausgaben zu überprüfen, die Genauigkeit durch bessere Prompts oder Daten zu verbessern), kann die Akzeptanz stagnieren.
- **Mangel an Bewusstsein oder Vorstellungskraft:** Einige Benutzer verstehen möglicherweise nicht, was Copilot über grundlegende Beispiele hinaus tun kann. Sie **realisieren einfach nicht**, dass bestimmte mühsame Aufgaben durch Copilot erleichtert werden könnten. Dies beschränkt die Nutzung auf einen engen Satz von Szenarien und lässt potenzielle Vorteile auf dem Tisch liegen.
- **Informationssilos/Kommunikation:** In einer großen Organisation hört nicht jeder die gleiche Botschaft. Es ist möglich, dass einige Teams kaum wussten, dass Copilot verfügbar war oder dass es auf mehr Apps erweitert wurde. Eine konsistente, wiederholte Kommunikation ist herausfordernd, aber unerlässlich – eine einzige All-Hands-Ankündigung reicht nicht aus.
- **Unterstützung im großen Maßstab:** Wenn Hunderte von Benutzern anfangen, Copilot auszuprobieren, werden sie Fragen haben oder Hilfe benötigen. Der übliche Helpdesk hat möglicherweise nicht alle Antworten, wenn er nicht in Copilot-Nutzungsfragen geschult ist („Die Zusammenfassung war nicht korrekt – was mache ich?" ist kein typisches IT-Ticket). Die Einrichtung eines Support-Modells für die Akzeptanz (das Power-User als Ersthelfer einbezieht usw.) ist eine Herausforderung, die die Sitzung mit Champion-Programmen ansprach.

Werkzeuge & Methoden:

Um diese Herausforderungen zu überwinden, teilte die Sitzung eine Vielzahl von Akzeptanztaktiken und -ressourcen – im Grunde ein Toolkit für das Change Management im KI-Kontext:

- **Kommunikationskampagne:** Starten Sie eine nachhaltige interne Marketingkampagne für Copilot. Nicht nur eine E-Mail, sondern eine Reihe von Kommunikationen:

    - **Unterstützung durch die Führung:** Eine Nachricht oder ein kurzes Video von einem leitenden Angestellten (z. B. CIO oder COO), das hervorhebt, warum das Unternehmen Copilot implementiert („um Sie von der Plackerei zu befreien, damit Sie sich auf hochwertige Arbeit konzentrieren können“) und Vertrauen in die Fähigkeit der Mitarbeiter ausdrückt, es zu nutzen. Dies setzt einen positiven Ton von oben.
    - **Erfolgsgeschichten:** Sobald erste Benutzer Erfolge melden, teilen Sie sie. Z. B. „Team A hat die Vorbereitungszeit für Berichte um 30 % mit Copilot verkürzt – hier ist, wie es ihnen geholfen hat, eine knappe Frist einzuhalten.“ Menschen lieben Geschichten; es hilft Skeptikern, praktische Möglichkeiten zu sehen.
    - **FAQs und Mythenaufklärung:** Sprechen Sie proaktiv häufige Bedenken an. Zum Beispiel könnte ein Q&A klarstellen: „Nein, Copilot ersetzt keine Arbeitsplätze – es ist ein Werkzeug, um Ihre Expertise zu erweitern“ oder „Copilot hat nur Zugriff auf die Daten, für die Sie bereits eine Berechtigung haben.“ Das Zerstreuen von Ängsten schafft Vertrauen.
    - **Multichannel-Outreach:** Nutzen Sie E-Mail, das Intranet, Yammer/Viva Engage-Posts, digitale Beschilderung, sogar physische Poster, falls relevant („Haben Sie Copilot in Outlook ausprobiert? Es kann Antworten sofort entwerfen!“). Wiederholung über Kanäle hinweg stellt die Reichweite sicher.
- **Schulungsprogramme:** Bieten Sie gestaffelte Schulungen an, um unterschiedlichen Lernpräferenzen gerecht zu werden:
    - **Kurze How-To-Videos:** Demonstrieren Sie eine Funktion in 2-3 Minuten (z. B. „Copilot verwenden, um ein Dokument zusammenzufassen“). Eine Bibliothek dieser mundgerechten Videos kann im Intranet oder im Lernmanagementsystem zur Verfügung gestellt werden. Mitarbeiter können bei Bedarf on-demand zusehen.
    - **Interaktive Workshops:** Veranstalten Sie Live-Schulungen (virtuell oder persönlich), bei denen ein Trainer mehrere Szenarien mit Copilot durchgeht und die Teilnehmer mitmachen oder Fragen stellen können. Dies abteilungsweise zu tun, kann es dem Trainer ermöglichen, relevante Beispiele zu verwenden (wie marketingbezogene Aufgaben für das Marketingteam usw.).
    - **Praktische Übungen:** Richten Sie nach Möglichkeit eine Sandbox-Umgebung mit Dummy-Daten ein, in der Mitarbeiter Copilot frei üben können, ohne sich Sorgen machen zu müssen, echte Arbeit durcheinanderzubringen. Geführte Laborübungen (mit schriftlichen Schritten zum Ausprobieren von Funktionen) können Vertrauen aufbauen.

    - **Spickzettel und Tipps:** Stellen Sie Kurzanleitungen (One-Pager) mit Beispielen für nützliche Prompts oder Befehle und Best Practices zur Verfügung. Z. B. „Wenn Sie Copilot bitten, eine E-Mail zu entwerfen: 1) geben Sie den Ton an (freundlich/formal), 2) erwähnen Sie wichtige Punkte, 3) lesen Sie den endgültigen Text immer Korrektur, bevor Sie ihn senden.“ Dies erinnert die Benutzer daran, wie sie effektiv mit dem Werkzeug interagieren können.
- **Champion-Programm und Community of Practice:** Nutzen Sie die natürlichen Enthusiasten – diejenigen, die früh den Wert erkennen und zu Power-Usern werden. Bilden Sie eine **Copilot-Champions-Gruppe**. Geben Sie ihnen zusätzliche Schulungen, damit sie anderen helfen können. Vielleicht nominiert jede Abteilung einen Champion.
    - Lassen Sie Champions „Sprechstunden“ oder Mini-Kliniken für ihre Kollegen veranstalten („Kommen Sie am Freitag an meinen Schreibtisch oder nehmen Sie an meinem Teams-Anruf teil, und ich helfe Ihnen, Copilot einzurichten oder ein Problem damit anzugehen“).
    - Ermutigen Sie Champions, fortgeschrittene Tipps in internen Foren zu teilen und ihre Beiträge zu feiern. Wenn beispielsweise ein Champion eine großartige Prompt-Technik herausfindet, um bessere Ergebnisse zu erzielen, wird dieser Tipp über das Intranet an alle Benutzer weitergegeben.
    - Erkennen Sie Champions in internen Newslettern oder bei Veranstaltungen an, um sie und andere zu motivieren. Eine Kultur, in der Kollegen als Anlaufstellen angesehen werden, beschleunigt die Akzeptanz organischer als die alleinige Abhängigkeit vom IT-Support.
- **Benutzer-Feedbackschleifen:** Bieten Sie einfache Möglichkeiten für Benutzer, Feedback zur Copilot-Nutzung zu geben, und stellen Sie sicher, dass das Feedback gehört und darauf reagiert wird:
    - **Feedback-Button im Werkzeug:** Aktivieren Sie nach Möglichkeit den integrierten Feedback-Mechanismus von Copilot (der Feedback an Microsoft sendet und auch an Ihr Admin-Dashboard weitergeleitet werden kann). Ermutigen Sie die Benutzer, ihn zu verwenden, wann immer die Ausgabe von Copilot nicht hilfreich oder besonders gut ist. Dies hilft, das Produkt im Laufe der Zeit zu verbessern (die KI lernt aus dem Feedback) und warnt Admins vor Problemstellen.
    - **Umfragen:** Senden Sie regelmäßig (sagen wir nach 1 Monat Nutzung, dann nach 3 Monaten) eine kurze Umfrage, in der Sie fragen, wie Copilot geholfen hat, welche Aufgaben am nützlichsten/wenigsten nützlich sind und welche Vorschläge es gibt. Dies sammelt nicht nur die Stimmung, sondern kann auch neue Anwendungsfälle aufdecken, die beworben werden können, oder Schulungsbedarf identifizieren („70 % der Befragten

wussten nicht, dass Copilot X tun kann – lassen Sie uns diese Funktion bekannt machen“).
    - **Fokusgruppen:** Treffen Sie sich mit kleinen Benutzergruppen aus verschiedenen Abteilungen, um ihre Erfahrungen zu diskutieren. Dieser qualitative Ansatz kann nuancierte Probleme oder brillante Ideen aufdecken. Z. B. könnte eine Fokusgruppe ergeben, dass Ingenieure Copilot großartig finden, um technische Spezifikationen zusammenzufassen, aber sich wünschen, dass es sich in ihr Code-Repository integrieren ließe – eine Erkenntnis, die ein zukünftiges Integrationsprojekt leiten könnte.
- **Teilen von Best Practices:** Erstellen Sie eine interne Wissensdatenbank mit **Copilot Best Practices**. Füllen Sie sie mit Inhalten, die von Champions, Early Adopters und Microsofts Anleitungen stammen:
    - **Do's and Don'ts-Liste** (z. B. „Zerlegen Sie komplexe Anfragen in kleinere“, „Fügen Sie keine sensiblen Informationen in einen Prompt ein“).
    - **Effektive Prompt-Beispiele** für gängige Aufgaben („Um einen guten ersten Entwurf zu erhalten, versuchen Sie, Ihre Anfrage so zu formulieren…“).
    - **Fehlerbehebung bei häufigen Problemen** („Wenn Copilot veraltete Informationen zu referenzieren scheint, versuchen Sie, auf ‚Webergebnisse einbeziehen‘ zu klicken oder zu prüfen, ob die verwendete Datei aktuell ist.“).

Diese Wissensdatenbank kann ein lebendiges Dokument sein, das aktualisiert wird, wenn neue Best Practices auftauchen. Bewerben Sie es über die oben genannten Community-Kanäle.

- **Verknüpfung der Akzeptanz mit Leistungszielen:** In einigen Organisationen könnte das Management sanfte Erwartungen setzen, dass Mitarbeiter zumindest versuchen, neue Werkzeuge zu integrieren. Zum Beispiel könnte ein Manager das Ziel haben, „die Teameffizienz durch die Nutzung digitaler Assistenten (Copilot) in vierteljährlichen Projekt-Workflows zu verbessern.“ Dies soll die Leute nicht hart unter Druck setzen, sondern signalisieren, dass die Führung die Akzeptanz schätzt. Es ermutigt mittlere Manager, die Copilot-Nutzung in ihren Teambesprechungen zu diskutieren („Wie können wir Copilot im nächsten Sprint verwenden?“). Die Einbettung in Leistungsdialoge kann die Nutzung beschleunigen (solange es positiv und nicht strafend formuliert ist).

Best Practices:

- **Normalisieren Sie die Nutzung von Copilot:** Ermutigen Sie Führungskräfte und Manager, bei der Nutzung von Copilot „mit gutem Beispiel voranzugehen“. Wenn ein Teamleiter in einem Meeting zeigt: „Ich habe Copilot verwendet, um unseren Projektplan zu entwerfen – lassen Sie uns ihn überprüfen“, entstigmatisiert das die KI-Unterstützung. Im Gegenteil, wenn Mitarbeiter das Gefühl haben, dass ihr Chef erwartet, dass alles von Hand gemacht wird, könnten sie die KI-Nutzung verbergen oder vermeiden. Die Unterstützung auf allen Ebenen, dass die Nutzung von Copilot kluge Arbeit und nicht faule Arbeit ist, ist entscheidend für die kulturelle Akzeptanz.
- **Respektieren Sie unterschiedliche Geschwindigkeiten:** Einige Mitarbeiter werden sofort einsteigen; andere werden zögern. Es ist wichtig, Spätadopter nicht zu beschämen oder ihnen das Gefühl zu geben, unzulänglich zu sein. Bieten Sie stattdessen weiterhin Hilfe an und heben Sie hervor, wie ihre Kollegen profitiert haben. Manchmal bewirkt eine persönliche Unterstützung Wunder („Hey, ich habe bemerkt, dass du Copilot noch nicht ausprobiert hast. Kann ich dir zeigen, wie ich es für E-Mails verwende? Es hat mir eine Menge Zeit gespart.“). Wenn Champions oder Teamleiter diese sanften Outreach-Bemühungen durchführen, können sie zögerliche Benutzer überzeugen.
- **Sammeln Sie Erfolgsmetriken zu Akzeptanzinitiativen:** Genauso wie wir die technische Nutzung von Copilot messen, messen Sie auch die Akzeptanzprogramme. Verfolgen Sie die Teilnahme an Schulungen, die Beteiligung in Communities und die Korrelation dieser mit Nutzungssteigerungen. Wenn beispielsweise nach einer Schulungssitzung die aktiven Benutzer im Team von 50 % auf 65 % gestiegen sind, funktioniert diese Methode – machen Sie mehr davon. Wenn eine bestimmte Abteilung trotz Outreach immer noch eine geringe Nutzung aufweist, ist vielleicht ein anderer Ansatz erforderlich (vielleicht ist ihre Arbeit nicht für die derzeit verfügbaren Copilot-Funktionen geeignet, was auch wertvolles Feedback für die zukünftige Entwicklung von KI-Fähigkeiten ist).
- **Kontinuierliche Kommunikation:** Die Akzeptanz ist kein einmaliger Vorstoß. Planen Sie laufende Kommunikationen: Heben Sie neue Funktionen hervor, wenn sich Copilot weiterentwickelt, teilen Sie vierteljährliche Nutzungs-Erfolgsstatistiken („zusammen haben wir in diesem Quartal 5.000 Stunden gespart – Kudos!“), aktualisieren Sie Schulungsmaterialien bei Bedarf. Neue Mitarbeiter sollten im Rahmen des Onboardings eine Copilot-Schulung erhalten. Halten Sie einen Rhythmus aufrecht, damit Copilot sichtbar und ermutigt bleibt, anstatt nach der anfänglichen Aufregung zu verblassen.
- **Gehen Sie konstruktiv mit negativem Feedback um:** Wenn einige Mitarbeiter kritisch sind („Copilot gibt mir generische Ausgaben“ oder „Es macht manchmal Fehler, ich vertraue ihm nicht“), weisen Sie dies nicht zurück – nutzen Sie es.

Untersuchen Sie, ob das Problem behebbar ist (vielleicht werden bessere Trainingsdaten oder eine Prompt-Anpassung benötigt) und lassen Sie sie wissen, dass ihr Feedback zu einer Verbesserung geführt hat. Verwalten Sie auch die Erwartungen: Klären Sie, dass Copilot ein Assistent ist, kein Orakel, und eine gewisse Iteration normal ist. Verstärken Sie die Gewohnheit, KI-Ausgaben zu überprüfen. Im Laufe der Zeit, wenn sich die KI verbessert und die Benutzer lernen, wie man sie verwendet, sollten diese negativen Fälle abnehmen. Zeigen Sie den Skeptikern den Trend, wenn möglich („Ja, in Woche 1 war die Fehlerrate X, aber in Woche 4 sank sie auf Y, nachdem wir Verbesserungen vorgenommen hatten – es wird besser, geben Sie ihm eine weitere Chance.“).

Letztendlich geht es bei **erfolgreicher Akzeptanz um Menschen, nicht um Technologie**. Durch die Schaffung einer unterstützenden Umgebung, die Bereitstellung von Lernressourcen und das aktive Management des Wandels können Entscheidungsträger sicherstellen, dass Copilot zu einem natürlichen Teil des Arbeitsablaufs der Mitarbeiter wird. Wenn sich die Mitarbeiter mit dem Werkzeug sicher fühlen und sehen, dass es ihnen hilft zu glänzen (nicht sie zu ersetzen), werden sie es selbst fördern. Die Organisation erntet dann die vollen Früchte ihrer Investition: eine Belegschaft, die nicht nur mit einem leistungsstarken KI-Werkzeug ausgestattet ist, sondern es tatsächlich nutzt, um jeden Tag mehr zu erreichen.

10. Kontinuierliche Verbesserung und nächste Schritte – Schritt halten mit der KI-Evolution

Die letzte Sitzung rundete die Deep-Dive-Veranstaltung mit einer zukunftsorientierten Perspektive ab. Die Bereitstellung von Copilot und sogar das Erreichen einer guten Akzeptanz ist nicht das Ende der Reise – es ist der Beginn eines neuen Modus der **kontinuierlichen Verbesserung**. KI-Fähigkeiten werden sich weiterentwickeln, die Bedürfnisse der Benutzer werden wachsen, und das Unternehmen muss seine Copilot-Bereitstellung kontinuierlich verfeinern. Entscheidungsträger erhielten Anleitungen, wie sie den Schwung aufrechterhalten, zukünftige Fortschritte integrieren und eine langfristige „Learn-it-all"-Kultur (wie Microsoft sie oft fördert) rund um KI pflegen können.

Bedeutung für Entscheidungsträger:

Dieser Abschnitt handelt im Wesentlichen von **Governance und Strategie als fortlaufendem Prozess**. Er ist wichtig, weil:

- **KI-Technologie ändert sich schnell:** Neue Funktionen (wie Copilot in neuen Apps oder verbesserte Modellversionen) werden weiterhin kommen. Die Organisation sollte einen Plan haben, um diese sicher zu pilotieren und einzuführen, anstatt überrumpelt zu werden oder auf einer älteren Version zu stagnieren.
- **Benutzerbedürfnisse entwickeln sich:** Wenn Mitarbeiter mit Copilot geschickter werden, werden sie neue Anwendungsfälle und auch neue Einschränkungen finden. Ein kontinuierlicher Feedback-Kanal stellt sicher, dass die Organisation reagieren kann – vielleicht durch die Aktivierung zusätzlicher Funktionen, das Hinzufügen von Datenquellen oder die Bereitstellung zusätzlicher Schulungen für fortgeschrittene Szenarien.
- **Skalierung und Verbreitung:** Nach der ersten Einführung in bestimmten Abteilungen oder Regionen könnten Entscheidungsträger planen, auf andere zu skalieren. Ein schrittweiser Ansatz mit Iteration bedeutet, dass jede Welle von der letzten lernen kann. Auch wenn das Unternehmen wächst (neue Akquisitionen, neue Mitarbeiter), muss das Copilot-Programm diese Personen an Bord holen und neue Inhaltsbereiche abdecken.
- **Im Einklang mit der Compliance bleiben:** Gesetze und Vorschriften können sich ändern. Was heute als akzeptable KI-Nutzung galt, muss morgen möglicherweise aufgrund regulatorischer Verschiebungen oder neuer ethischer Richtlinien angepasst werden. Eine statische Richtlinie riskiert, veraltet zu sein; ein lebendiger Governance-Prozess bleibt aktuell.

- **ROI kontinuierlich maximieren:** Kontinuierliche Verbesserung stellt sicher, dass Sie den maximalen Wert herausholen. Zum Beispiel könnten Analysen zeigen, dass eine Abteilung bei den Produktivitätsgewinnen zurückbleibt; gezielte Verbesserungsbemühungen dort (vielleicht die Anpassung von Copilot an ihren einzigartigen Arbeitsablauf) könnten zusätzlichen ROI freisetzen. Ohne kontinuierliche Bewertung werden diese Möglichkeiten verpasst.

Herausforderungen:

Kontinuierliche Verbesserung im Kontext von Unternehmens-KI hat ihre eigenen Herausforderungen:

- **Überwachungsmüdigkeit:** Nach der anfänglichen Projektphase könnten sich die Teams zerstreuen. Einen engagierten Fokus auf Copilot (über ein Center of Excellence oder ähnliches) aufrechtzuerhalten, erfordert nachhaltige Unterstützung durch die Führung. Es besteht das Risiko, dass, sobald „es bereitgestellt ist“, jeder zum nächsten Projekt übergeht und niemand mehr aktiv den Garten pflegt.
- **Einbeziehung von Benutzerfeedback im großen Maßstab:** Feedback einzuholen ist eine Sache; tatsächlich potenziell Tausende von Eingaben zu verarbeiten, sie zu priorisieren und in Aktionspunkte umzuwandeln, ist schwierig. Es erfordert einen Workflow und möglicherweise Werkzeuge (z. B. Feedback per KI kategorisieren, ha!). Viele Organisationen haben Schwierigkeiten, die Feedbackschleife zu schließen, sodass die Benutzer das Gefühl haben, ihre Vorschläge landen in einem schwarzen Loch.
- **Ressourcenzuweisung:** Kontinuierliche Verbesserung impliziert laufende Anstrengungen – was die Zeit von Menschen und vielleicht auch Budget bedeutet (für Auffrischungsschulungen, für die Beauftragung von Beratern für fortgeschrittene Modellabstimmung usw.). Entscheidungsträger müssen diese Ressourcen über das anfängliche Implementierungsbudget hinaus rechtfertigen und zuweisen.
- **Mit den Updates von Microsoft Schritt halten:** Microsoft wird Copilot kontinuierlich aktualisieren (neue Funktionen, bessere Modelle, Integration mit neuen Systemen). Einige Updates erfordern eine Aktion des Tenant-Admins, um sie zu aktivieren oder zu konfigurieren. Wenn der Admin nicht auf Ankündigungen achtet oder neue Funktionen nicht testet, könnte die Organisation zurückbleiben oder die Aktivierung von etwas Nützlichem verpassen. Umgekehrt könnte ein Update Auswirkungen haben, die Kommunikation oder eine Richtlinienanpassung erfordern (z. B. wenn Copilot eine neue Fähigkeit zum Erstellen von PowerPoint-Folien erhält, könnte ein Missbrauchsrisiko bestehen, für das Sie eine neue Richtlinie benötigen).

- **Messung der langfristigen Auswirkungen:** Anfänglich zeigen Metriken Akzeptanz und direkte Produktivität. Im Laufe der Zeit könnten die großen Gewinne bereits erzielt sein – weitere inkrementelle Verbesserungen könnten subtil sein. Die Organisation sollte versuchen, die KI-Nutzung mit **höherrangigen Ergebnissen** (wie Innovationsrate, Mitarbeiterengagement, Kundenzufriedenheit) zu verbinden. Dies ist schwer zu messen, aber die Grenze des Nachweises des KI-Werts.

Werkzeuge & Methoden:

Die Sitzung bot wahrscheinlich einen Fahrplan zur Aufrechterhaltung eines effektiven Copilot-Programms. Wichtige Werkzeuge und Methoden umfassen:

- **Copilot Control System Committee (Operative Kadenz):** Übergang vom Projektmodus zur dauerhaften Governance. Vielleicht trifft sich das funktionsübergreifende Governance-Board, das den Rollout gesteuert hat, weiterhin monatlich oder vierteljährlich. Agenda: Überprüfung der neuesten Nutzungsmetriken, Überprüfung von Vorfällen (Sicherheit oder Benutzerprobleme), Diskussion anstehender Änderungen (intern oder von Microsoft) und Planung erforderlicher Maßnahmen (wie eine neue Schulung, wenn eine neue Funktion eintrifft). Die Aufrechterhaltung dieses Komitees stellt eine kontinuierliche Abstimmung sicher.
- **Informiert bleiben über Microsoft-Ressourcen:** Weisen Sie jemanden (einen „CoPilot Product Champion“ in der IT oder im CoE) zu, um die Updates, die Roadmap und die Community-Diskussionen von Microsoft zu verfolgen. Sie können die Microsoft 365 Roadmap abonnieren, an Webinaren teilnehmen oder der Tech-Community folgen (wie der, auf der die Veranstaltung gehostet wurde). Wenn Microsoft beispielsweise ankündigt: „Copilot integriert sich jetzt in Wissensdatenbanken von Drittanbietern“ oder „Neue Compliance-Zertifizierungen erreicht“, bringt dieser Champion die Nachrichten in das Komitee, um zu entscheiden, ob/wie man sie nutzt. Dieser proaktive Ansatz vermeidet, hinterherzuhinken oder kritische Updates zu verpassen (die letzte Sitzung der Veranstaltung wies auf Ressourcen wie die Tech Community für kontinuierliches Lernen hin).
- **Kontinuierliche Schulung & Kompetenzaufbau:** Erkennen Sie an, dass die Beherrschung von Copilot sich im Laufe der Zeit entwickeln wird. Bieten Sie einige Monate später **fortgeschrittene Schulungen** an („Steigern Sie Ihre Copilot-Fähigkeiten – Fortgeschrittene Tipps und Tricks“), damit Benutzer, die die Grundlagen beherrschen, anspruchsvollere Anwendungen lernen können (wie das Verketten mehrerer Copilot-Ergebnisse, um eine komplexe Aufgabe zu erledigen). Aktualisieren Sie Schulungsmaterialien und Best-Practice-

Anleitungen, wenn neue Funktionen eingeführt werden (z. B. wenn sich das Verhalten der Websuche ändert oder neue Datenschutzkontrollen eingeführt werden, integrieren Sie diese schnell in die Benutzeranleitung). Die Orientierung für neue Mitarbeiter sollte eine Copilot-Schulung beinhalten – möglicherweise sogar die Zuweisung eines „Copilot-Buddys“ (ein Teammitglied, das ein erfahrener Benutzer ist), um sie in ihrer spezifischen Rolle auf den neuesten Stand zu bringen.

- **Richtlinien und Einstellungen basierend auf Daten weiterentwickeln:** Nutzen Sie Analysen und Feedback-Trends zur Feinabstimmung. Wenn beispielsweise nach 6 Monaten 95 % der Copilot-Nutzung von einer Abteilung stammen und eine andere sie kaum nutzt, untersuchen Sie, warum – vielleicht ist der Inhalt der zweiten Abteilung nicht integriert. Planen Sie, ihren Inhalt in den Index von Copilot aufzunehmen oder einen neuen Akzeptanz-Push in dieser Abteilung durchzuführen. Wenn Sicherheitsprotokolle null Vorfälle für eine bestimmte, anfangs blockierte Funktion zeigen, erwägen Sie, sie kontrolliert zu aktivieren, um den Nutzen zu erhöhen. Pflegen Sie ein **lebendiges Richtliniendokument**, das versioniert wird. Stellen Sie sicher, dass Änderungen kommuniziert werden – z. B. „Ab nächstem Monat wird die Copilot-Websuche für alle Benutzer aktiviert, da unsere Tests gezeigt haben, dass sie die Compliance aufrechterhält (siehe neue Richtlinien im Anhang).“
- **Periodische Erfolgs-Neubewertung (ROI-Präsentationen):** Führen Sie nach, sagen wir, einem Jahr eine gründliche Bewertung der Auswirkungen von Copilot durch. Dies könnte eine Fortsetzung des anfänglichen KPI-Trackings sein, aber auch breitere Ergebnisse einbeziehen: Haben sich die Mitarbeiterengagement-Scores geändert? Sind die Produktentwicklungszyklen kürzer? Hat sich das Kundenfeedback verbessert, weil die Mitarbeiter schneller oder konsistenter antworten? Auch wenn die Korrelation schwer endgültig zu beweisen ist, sammeln Sie so viele Beweise wie möglich (quantitativ und qualitativ). Erstellen Sie einen Bericht für die oberste Führungsebene, der die Ergebnisse des ersten Jahres und die Pläne für das zweite Jahr zusammenfasst (wie die Erweiterung auf neue Szenarien oder weitere Schulungen). Der Nachweis eines nachhaltigen Werts in geschäftlicher Hinsicht sichert die fortgesetzte Unterstützung und Finanzierung für Copilot-bezogene Verbesserungen.
- **Plan für Modell-/Daten-Updates:** Entwickeln Sie einen **Wartungskalender**. Zum Beispiel:
    - **Vierteljährlich:** Überprüfen und aktualisieren Sie den Wissensdatenbankinhalt, aus dem Copilot schöpft (z. B. die neuesten Q&As hinzufügen, veraltete Informationen entfernen).

    - **Halbjährlich:** Wenn neue LLM-Modelle verfügbar sind (mit besserer Leistung oder Kosteneffizienz), bewerten Sie sie in einem Pilotprojekt und entscheiden Sie über einen Wechsel.
    - **Jährlich:** Bewerten Sie neu, welche neuen Prozesse im Unternehmen von Copilot profitieren könnten, die anfangs nicht im Geltungsbereich waren. Das Geschäft entwickelt sich weiter – vielleicht wurde eine neue Abteilung gegründet, die jetzt ihre eigene Copilot-Lösung erstellen könnte. Starten Sie eine neue Deep-Dive- oder Design-Thinking-Sitzung mit ihnen.
- **Nutzen Sie Microsofts „Copilot Adoption Hub“:** Die Sitzung verwies auf Ressourcen wie den „M365 Copilot Adoption Hub“ und die „Leading in the Era of AI“-Website. Weisen Sie den Akzeptanzleiter oder das CoE-Team an, diese regelmäßig für frische Ideen zu besuchen – Microsoft und die Community werden Erfolgsgeschichten, neue Toolkit-Elemente und aufkommende Best Practices teilen, während mehr Organisationen Copilot ausrollen. Integrieren Sie nützliche in Ihr Programm. Im Wesentlichen lernen Sie weiterhin von der breiteren Community, damit Ihre Praktiken auf dem neuesten Stand bleiben.

Best Practices:

- **Meilensteine feiern & Wertschätzung zeigen:** Wenn das Unternehmen Akzeptanzziele erreicht oder ein Jahr erfolgreicher Nutzung feiert, feiern Sie es. Dies könnte eine kleine interne Kampagne sein („1 Jahr mit Copilot – Das haben wir erreicht“). Erkennen Sie wichtige Beitragende an (IT-Team, Champions, hoch-adoptierende Abteilungen). Dies erhält die Moral und den Schwung.
- **Das Gespräch am Laufen halten:** Ermutigen Sie die Mitarbeiter, ihre Copilot-Erfahrungen weiterhin in internen Foren zu teilen. Starten Sie vielleicht einen monatlichen internen Newsletter-Schnipsel: „Copilot Corner – Tipp des Monats“ oder eine kurze Geschichte von einem Benutzer. Die KI im Gespräch zu halten, hilft, sie als normalen Teil des Arbeitslebens zu normalisieren (wie E-Mail oder Teams). Es deckt auch laufende Probleme oder Wünsche auf, die die kontinuierliche Verbesserung speisen können.
- **Organisatorische Richtlinien nach Bedarf anpassen:** Wenn KI verankert wird, müssen möglicherweise einige organisatorische Richtlinien oder Rollen aktualisiert werden. Zum Beispiel könnte die Richtlinie zur akzeptablen Nutzung bis zum Jahresende eine KI-Klausel erhalten („Von Mitarbeitern wird erwartet, dass sie KI-Werkzeuge ethisch und verantwortungsbewusst verwenden, z. B. Ausgaben überprüfen, keine eingeschränkten Daten über das Erlaubte hinaus eingeben.“). Oder vielleicht entsteht eine neue Rolle, wie ein „KI-Systemmanager“ in der IT oder jede Geschäftseinheit benennt einen „KI-Botschafter“. Seien Sie offen für die Schaffung dieser Rollen oder Regeln,

während die Rolle der Technologie reift. Behandeln Sie Copilot im Wesentlichen nicht als Pilotprogramm, sondern als festen Bestandteil des Tech-Ökosystems, was Änderungen in der Arbeitsweise und Organisation der Menschen mit sich bringen kann.

- **Agil und aufgeschlossen bleiben:** Die Reise endet nicht – es wird immer einen nächsten Schritt geben. Die heutige Best Practice könnte sich morgen weiterentwickeln. Verankern Sie eine agile Denkweise auf Führungsebene: Überprüfen Sie die Ergebnisse, ändern Sie Strategien, wenn etwas nicht funktioniert (vielleicht ist ein Schulungsansatz nicht effektiv – versuchen Sie eine andere Methode), und experimentieren Sie mit neuen Funktionen oder Ansätzen in kleinem Maßstab, um zu sehen, ob sie breiter ausgerollt werden sollten. Dieser iterative, aufgeschlossene Ansatz stellt sicher, dass die Organisation im Laufe der Zeit einen steigenden Wert aus Copilot zieht, anstatt nach anfänglichen Gewinnen zu stagnieren.

Zusammenfassend lässt sich sagen, dass die Reise mit Microsoft 365 Copilot eine **fortlaufende Evolution** ist. Durch die Etablierung einer wachsamen Governance, die Förderung einer weit verbreiteten effektiven Nutzung und die Verpflichtung zu kontinuierlichem Lernen und Verbessern können Entscheidungsträger sicherstellen, dass Copilot ein dynamisches Gut für die Organisation bleibt. Das **Copilot-Kontrollsystem** ist also keine einmalige Einrichtung, sondern ein **lebendiges Rahmenwerk** – eines, das mit der Technologie und dem Unternehmen wächst und sich anpasst. Entscheidungsträger, die diese Denkweise annehmen, werden ihre Organisationen nicht nur dazu führen, die heutigen Gewinne aus Copilot zu erzielen, sondern diese Gewinne kontinuierlich zu verstärken, während sich sowohl die KI als auch die Geschäftslandschaft weiterentwickeln.

Schlussfolgerung:

Dieses Deep-Dive-Handbuch hat das gesamte Spektrum der **Sicherung, Verwaltung, Messung und Weiterentwicklung** der Copilot-Nutzung in einem Unternehmen durchlaufen. Indem wir die zehn Hauptfokusbereiche abgedeckt haben, haben wir veranschaulicht, wie ein Entscheidungsträger ein robustes Programm rund um Microsoft 365 Copilot aufbauen kann: von der Implementierung starker **Sicherheits- und Compliance-Kontrollen**, über die Etablierung von **Verwaltungspraktiken und Maker-Befähigung**, bis hin zur **Messung der Auswirkungen und Förderung der kontinuierlichen Akzeptanz**, bis hin zur Planung für die **zukünftigen Verbesserungen**.

Zusammenfassend sind die wichtigsten Erkenntnisse für Entscheidungsträger:

- **Schaffen Sie eine starke Grundlage mit klaren Governance-Säulen.** Sichern Sie Daten und wahren Sie die Compliance vom ersten Tag an durch Richtlinien und Aufsichtswerkzeuge, damit Sie KI zuversichtlich annehmen können.
- **Befähigen Sie Ihre Mitarbeiter zur Innovation, innerhalb eines geführten Rahmens.** Nutzen Sie Zonen und Umgebungskontrollen, um die Self-Service-Entwicklung zu ermöglichen und gleichzeitig Sichtbarkeit und Kontrolle zu behalten. Der Einfallsreichtum Ihrer Mitarbeiter wird die besten Anwendungsfälle aufdecken – fördern Sie ihn.
- **Messen Sie, was zählt.** Verfolgen Sie kontinuierlich Nutzung und Ergebnisse, um die Vorteile von Copilot zu quantifizieren, und nutzen Sie diese Erkenntnisse, um sowohl die Konfiguration des Werkzeugs als auch das Unterstützungsprogramm darum herum zu verfeinern.
- **Investieren Sie in Akzeptanz und Change Management.** Technologie allein transformiert keine Geschäftsprozesse – Menschen tun es. Schulen Sie sie, unterstützen Sie sie, hören Sie ihnen zu. Bauen Sie eine Kultur auf, die KI-Unterstützung als eine kluge Arbeitsweise fördert.
- **Setzen Sie die Reise fort.** Behandeln Sie die Bereitstellung von Copilot als ein lebendiges Programm. Aktualisieren Sie Richtlinien mit gewonnenen Erkenntnissen, rüsten Sie auf neue Funktionen auf und integrieren Sie Copilot tiefer, wo er Mehrwert schafft. Seien Sie bereit, sich anzupassen, wenn sich KI und Geschäftsanforderungen Hand in Hand entwickeln.

Indem sie die in diesem Handbuch beschriebenen Praktiken befolgen, können Entscheidungsträger sicherstellen, dass Microsoft 365 Copilot und verwandte KI-Agenten zu einem **vertrauenswürdigen, unverzichtbaren Verbündeten** in der Organisation werden – einer, der nicht nur kurzfristig Produktivität und Effizienz steigert, sondern auch eine langfristige Transformation der Arbeitsweise vorantreibt, alles unter sicheren und gut verwalteten Bedingungen. Das Ergebnis ist ein Unternehmen, das sowohl **leistungsstark als auch widerstandsfähig** ist und die Kraft der KI nutzt, während es die Werte von Sicherheit, Compliance und einer Lernkultur hochhält.