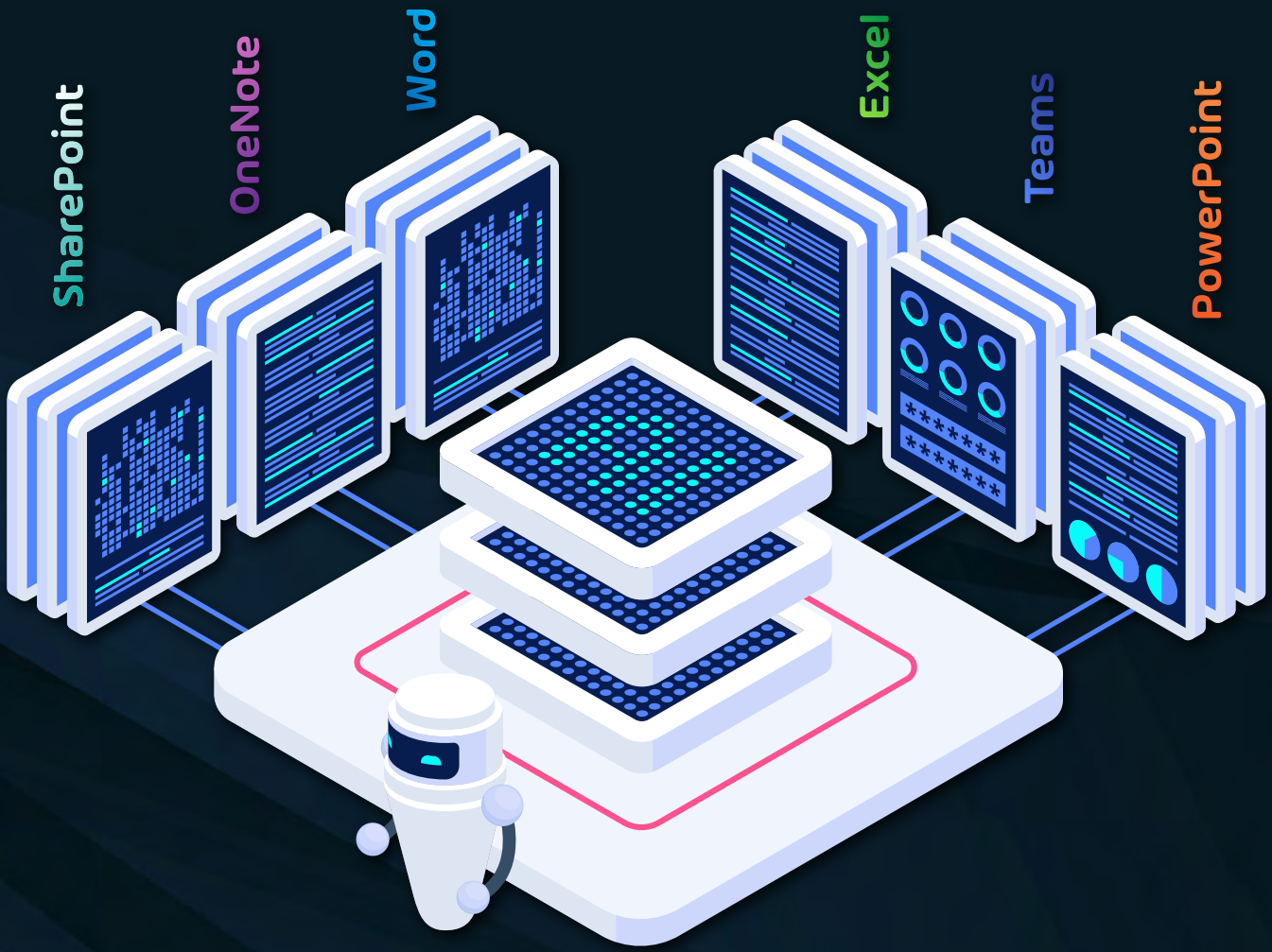
SO MACHEN SIE IHR UNTERNEHMEN MICROSOFT COPILOT-READY



HORNETSECURITY

SO MACHEN SIE IHR UNTERNEHMEN **MICROSOFT COPILOT-READY**

MICROSOFT 365-BERECHTIGUNGEN MANAGEN – DATENLECKS VERMEIDEN

Künstliche Intelligenz ist das Thema der Stunde und beeinflusst bereits die Art und Weise, wie wir arbeiten. So verspricht Microsoft Copilot den Arbeitsalltag der Mitarbeiter enorm zu erleichtern. Der digitale KI-Assistent kann beispielsweise Präsentationen gestalten, Zusammenfassungen erstellen oder E-Mails verfassen. Dafür greift Copilot auf dieselben Dokumente, E-Mails und Dateien in SharePoint und OneDrive von Microsoft 365 zu, auf die der Nutzer Zugriff hat, um individualisierte Ergebnisse zu liefern. Was auf den ersten Blick nach einer großen Arbeitserleichterung klingt, birgt auch ein großes Risiko: Sensible Daten können in die falschen Hände geraten! Ein Albtraum für CISOs und Administratoren.

Dieses Whitepaper befasst sich mit den Risiken, die mit der Nutzung von Copilot einhergehen und zeigt eine Lösung auf, wie ein effektives Berechtigungsmanagement implementiert werden kann, um Kontrollverlust zu verhindern und die Compliance sicherzustellen.

Copilot greift auf alle Daten in SharePoint zu, für die ein Benutzer eine Berechtigung hat.

DATENLECK-RISIKO DURCH COPILOT-SUCHE IN ONEDRIVE UND SHAREPOINT

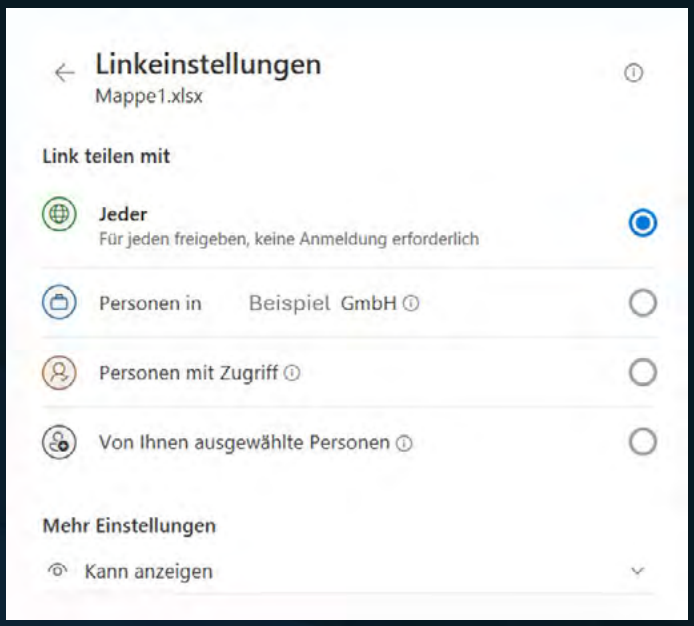
Die mögliche Arbeitserleichterung durch Copilot ist vielfältig. So kann das Tool mittels sogenannter Prompts, also vom Nutzer verfasster Befehle, Informationen zusammenfassen, bearbeiten oder kreativ aufbereiten.

Zur Informationsbeschaffung greift Copilot auf die Inhalte aller Microsoft 365 Anwendungen wie Word, Excel, PowerPoint, Outlook und Teams zu. Der KI-Assistent kann in Sekundenschnelle Daten aus den Dokumenten, Excel-Tabellen, Präsentationen, etc., die in SharePoint und OneDrive liegen, zusammenstellen.

Da Copilot bei der Recherche auf alle Daten zugreift, für die ein Nutzer über eine Berechtigung verfügt, kann es passieren, dass das Tool auf sensible Informationen (personenbezogene Daten, sicherheitsrelevante Informationen, Geschäftszahlen, Gehaltsinformationen, etc.) in SharePoint oder OneDrive stößt, auf die der Nutzer eigentlich gar keinen Zugriff haben sollte, aufgrund von ungünstigen standardmäßigen Freigabekonfigurationen aber Zugangsberechtigungen vorliegen.

EIN BEISPIEL:

Ein Mitarbeiter teilt ein Excel-Dokument mit sensiblen Geschäftszahlen über die „Freigeben"-Funktion schnell und einfach per Link mit seinem Vorgesetzen. Problematisch wird es, wenn aufgrund der Standard-Freigabeeinstellung automatisch ein Zugangslink generiert wird, der jedem im Unternehmen oder, schlimmer noch, einfach jedem, der über diesen Link verfügt, Zugriff gewährt.



Auch wenn andere Mitarbeiter des Unternehmens nichts von dem Dokument wissen, und nicht diesen direkten Link erhalten, hat Copilot dennoch Zugriff darauf und kann Informationen aus dem Dokument auslesen und in Rechercheergebnisse von anderen Mitarbeitern einfließen lassen.

IN MICROSOFT TEAMS GETEILTE DOKUMENTE WERDEN IN SHAREPOINT GESPEICHERT

Das Teilen von Dateien in Teams erhöht ebenfalls das Risiko eines Datenlecks im Zusammenhang mit Copilot, wenn die Freigabeeinstellung nicht richtig konfiguriert sind. Was den wenigsten bewusst ist: Wenn eine Datei in einem Teams-Channel geteilt wird, wird sie in SharePoint gespeichert.

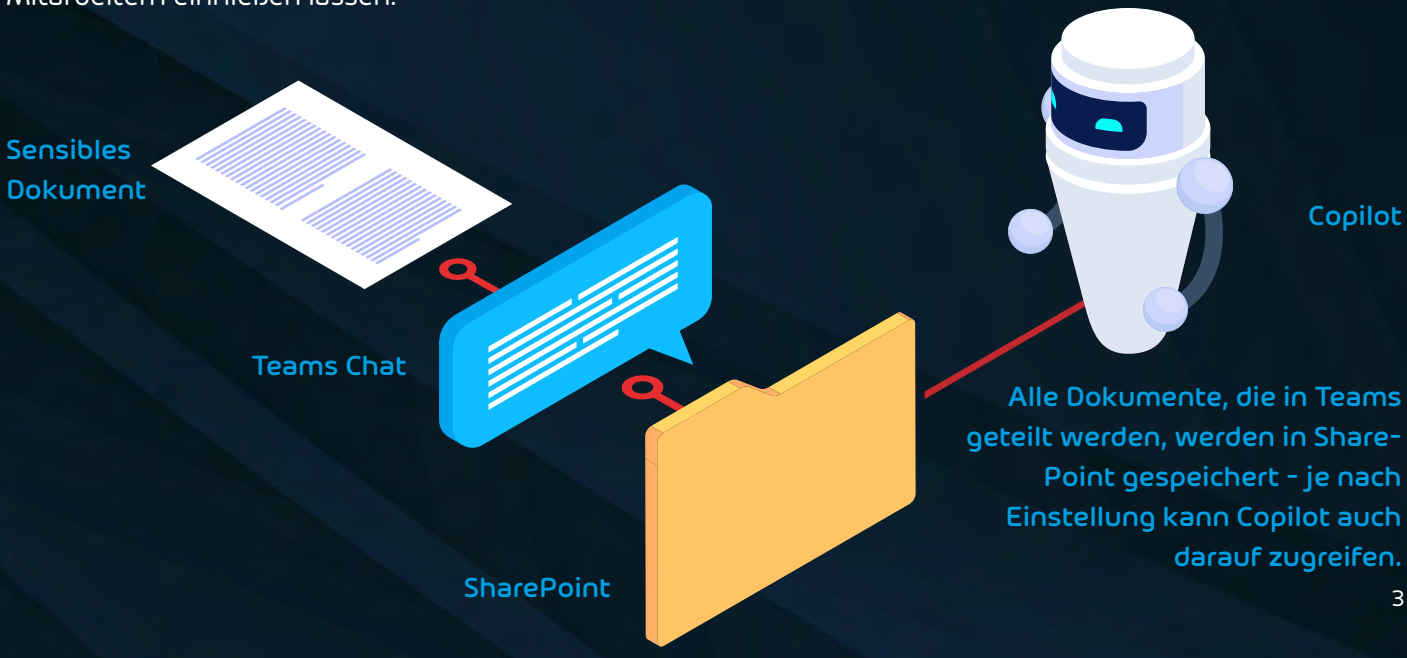
Dateien, die wiederum in einem Einzel- oder Gruppenchat hochgeladen werden, landen im Ordner „Microsoft Teams Chat-Dateien" des OneDrive for Business. Für private Channels wird sogar eine separate SharePoint-Site mit einer exklusiven Dokumentenbibliothek für die Mitglieder eingerichtet.

So werden alle Dokumente in verschiedenen SharePoint-Sites statt direkt in Teams gespeichert.

Auch hier kann eine Person mittels Copilot wie im zuvor beschriebenen Fall Zugriff auf die Inhalte bekommen, wenn diese Dateien standardmäßig beispielsweise einfach für „Jeden" freigegeben sind.

Besonders problematisch wird es, wenn externe Microsoft 365-Gastnutzer Copilot nutzen, um an Informationen von dem Unternehmen zu gelangen, auf die sie eigentlich keine direkten Zugriffslinks haben.

Für CISOs und Admins sollte das alarmierend sein.



STARKES BERECHTIGUNGSMANAGEMENT FÜR MICROSOFT 365-DATEN ERFORDERLICH

Copilot nutzt und zeigt alle Organisationsdaten an, für die einzelne Nutzer mindestens Anzeigeberechtigungen haben. Daher ist es wichtig, dass das Unternehmen das **Need-to-Know Prinzip**, also die Vergabe von minimalen Zugriffsrechten in Microsoft 365 strikt umsetzt.

Das bedeutet, Benutzern nur Zugriff auf die für ihre Arbeit erforderlichen Daten zu gewähren und keine darüberhinausgehenden Berechtigungen zu erteilen. Diese Zugriffsrechte sollten aktualisiert werden, wenn sich Benutzerrollen innerhalb der Organisation ändern.

Ein effizientes Berechtigungsmanagement ist auch aufgrund von Gesetzen und Regularien unabdingbar.

Wenn es um den Zugriff auf Unternehmensdaten geht, muss auch rechtlichen Anforderungen entsprochen werden. Diese richten sich nach verschiedenen Faktoren, wie z. B. den Unternehmensstandort und um welche Daten es sich handelt. Besonders seit NIS2 in Kraft getreten ist, hat auch die Branchenzugehörigkeit einen entscheidenden Einfluss auf den zukünftigen Aufwand für Admins und CISOs.

Mit den vorhandenen Microsoft-Tools ist es weder möglich, einen vollständigen Überblick über alle im Unternehmen vergebenen Berechtigungen zu erhalten, noch mandantenweit Freigabe-Richtlinien durchzusetzen und zu überwachen. Zudem betreffen Änderungen an den Einstellungen innerhalb der Microsoft-Tools lediglich Dateien, die ab dem Zeitpunkt der Änderung erstellt bzw. geteilt werden.

Eine reflexhafte Reaktion ist daher oft die komplette Dateifreigabe zu sperren oder keine externen Freigaben zuzulassen und für die internen Freigaben strenge Standardberechtigungen vorzugeben. Das wird allerdings dazu führen, dass die Benutzer nach einem anderen Weg suchen, Dateien auszutauschen. Sensible Dokumente werden dann möglicherweise über Cloud-Speicher von Drittanbietern oder per E-Mail freigegeben, in die CISOs und Admins noch weniger Einblick haben.

„RESTRICTED SHAREPOINT SEARCH"-SETTING VON MICROSOFT IST NICHT DIE LÖSUNG

Auch Microsoft selbst hat erkannt, dass es bei der Copilot-Recherche in SharePoint zu Problemen kommen kann. Im April 2024 hat das Unternehmen daher für Administratoren als Public Preview das "Restricted SharePoint Search" -Setting eingeführt. Damit kann die unternehmensweite Suche und die Copilot-Recherche auf ausgewählte SharePoint-Sites beschränkt werden.

Restricted SharePoint Search kann die Genauigkeit von Copilot-Antworten beeinflussen.

Hierbei handelt es sich allerdings um eine Funktionalität, die keinen Raum für granulare Einstellungen bietet. Entweder ist eine SharePoint-Site zugelassen oder sie ist komplett blockiert.

Die Aktivierung dieser Funktion hat also Auswirkungen auf das gesamte Sucherlebnis, auch für Nicht-Copilot-Benutzer. Copilot hat weniger Informationen zur Verfügung, was sich auf seine Fähigkeit auswirken kann, genaue und umfassende Antworten zu geben.

Für einen optimalen Copilot-Einsatz kann das also auch nicht die Lösung sein.

Um sicherzustellen, dass Dateien fortlaufend über die richtigen Berechtigungen verfügen und damit nur für den Nutzer vorgesehene Dateien in der Copilot-Recherche auftauchen, bedarf es einer Drittanbieter-Lösung, die effizientes Data Lifecycle Management im großen Maßstab für Microsoft 365 ermöglicht.

MIT 365 PERMISSION MANAGER COPILOT-READY WERDEN

Was zur Einhaltung von definierten Freigabe-Richtlinien dringend benötigt wird, ist ein skalierbares Tool, das selbst große Mandanten mit Tausenden von SharePoint-Sites mühelos abdeckt.

Mit 365 Permission Manager ist es möglich, effektiv Zugriffe und Berechtigungen zu überwachen und zu verwalten. Insbesondere mit Blick auf Copilot wird durch die Vereinfachung des Berechtigungsmanagements verhindert, dass sich Informationen ungewollt verbreiten.

Anstatt durch die verschiedenen Portale in den nativen Tools von Microsoft navigieren zu müssen, bietet der 365 Permission Manager für Admins und CISOs eine bequeme und benutzerfreundliche Oberfläche, um Berechtigungen in M365-Umgebungen umfassend zu überblicken, Compliance-Richtlinien zu definieren und Verstöße zu verhindern bzw. zu revidieren.

DIE VORTEILE VOM 365 PERMISSION MANAGER

Umfangreiches Monitoring

» Der 365 Permission Manager bietet einen vollständigen Überblick über die M365 Berechtigungen für SharePoint, OneDrive und Microsoft Teams. Eine erweiterte Filterfunktion zeigt, auf welche Elemente externe Benutzer oder Gäste zugreifen können. Des Weiteren werden Admins und CISOs benachrichtigt, wenn Dateien, Sites oder Ordner an externe Stakeholder freigegeben werden.

Benutzerdefinierte Berechtigungsrichtlinien

» Der 365 Permission Manager ermöglicht es, vorgefertigte Berechtigungsrichtlinien festzulegen und benutzerdefinierte Richtlinien zu erstellen. Diese können bedarfsgerecht auf Site-, Ordner- und Dateiebene angewendet werden. Damit unterscheidet er sich grundlegend von den 365 Microsoft Tools, die standardisierte Richtlinien vorgeben.

Berechtigungen im großen Maßstab verwalten

» Im Control Panel des 365 Permission Managers können Anpassungen in großem Umfang durchgeführt werden. Mit sogenannten Massenaktionen können Berechtigungen für beliebig viele Tenants und Gruppen zeitgleich angepasst werden. Das spart Zeit und Aufwand und gewährleistet eine Konformität bei den Berechtigungen der Mitarbeiter.

Stets die Kontrolle behalten

» Bei einem Verstoß erhalten der Admin oder CISO eine Warnmeldung. Dabei wird mitgeteilt, um welche User und Sites, Dateien oder Ordner es sich handelt. Das ermöglicht sofortiges Handeln, um Datenlecks zu verhindern. Verstöße können fallbasiert oder in Massenaktionen genehmigt oder abgelehnt werden.

» Ein besonders nützliches Feature ist die To-Do-Liste: Hier werden sämtliche Verstöße gegen die auf jeder SharePoint Online-Site angewendeten Richtlinien aufgelistet. Diese Verstöße können in großem Umfang korrigiert werden, bzw. Ausnahmen festgelegt werden, sofern eine geschäftliche Rechtfertigung besteht. Auch Mitarbeiter werden in die Verantwortung genommen. Per E-Mail erfahren sie von Richtlinien-Verstößen, die die OneDrive oder SharePoint-Sites betreffen, von denen sie Site-Owner sind.

Egal, ob es darum geht Berechtigungsrichtlinien einzuhalten, Informationen und Daten zu schützen oder auf die Nutzung von Copilot im Unternehmen vorbereitet zu sein, der 365 Permission Manager ist auf solche Anforderungen ausgelegt und CISOs und Administratoren können sich darauf freuen, Copilot auf eine sichere und konforme Weise einzusetzen.