Überschrift:

Microsoft Copilot: Warum KI eine saubere Berechtigungsstruktur braucht

Einführungstext:

Microsoft Copilot verändert, wie Anwender Informationen in Microsoft 365 finden und verarbeiten. Dadurch gewinnt eine bekannte Sicherheitsfrage zusätzlich an Bedeutung: Wer hat eigentlich Zugriff auf welche Daten? Vor dem KI-Rollout sollten Unternehmen deshalb nicht nur über die neue Technologie sprechen, sondern auch ihre bestehenden Berechtigungsstrukturen kritisch prüfen.

Text:

Microsoft Copilot ermöglicht es Anwendern, Informationen aus ihrer Microsoft-365-Arbeitsumgebung schneller zu finden, zusammenzufassen und miteinander in Beziehung zu setzen. Dabei gelten weiterhin die vorhandenen Zugriffsrechte: Ein Benutzer kann grundsätzlich nur auf Informationen zugreifen, für die er entsprechende Berechtigungen besitzt.

Genau hier liegt jedoch eine häufig unterschätzte Herausforderung. Microsoft-365-Umgebungen entwickeln sich über Jahre. Mitarbeiter wechseln Abteilungen, Projektgruppen entstehen und verschwinden, externe Partner werden eingebunden und Dokumente über SharePoint, OneDrive oder Teams geteilt. Hinzu kommen direkte Berechtigungen, Gruppenmitgliedschaften, verschachtelte Gruppen und Sharing Links. Das Ergebnis kann eine komplexe Berechtigungsstruktur sein, bei der kaum noch transparent ist, wer tatsächlich auf welche Informationen zugreifen kann.

Mit generativer KI verändert sich die Konsequenz solcher Fehlberechtigungen. Früher musste ein Mitarbeiter eine sensible Datei möglicherweise gezielt suchen oder zufällig entdecken. Copilot kann Informationen aus verschiedenen zugänglichen Quellen auffindbar machen und in einem neuen Kontext zusammenführen. Eine veraltete Berechtigung, die jahrelang unbemerkt blieb, kann dadurch plötzlich relevant werden. Das Sicherheitsproblem entsteht dabei nicht durch Copilot selbst – die zugrunde liegende Zugriffsberechtigung bestand bereits vorher.

Ein einfaches Beispiel: Ein Mitarbeiter wechselt vom Finance-Team in eine andere Abteilung, bleibt aber weiterhin Mitglied einer Gruppe mit Zugriff auf bestimmte Finanzdokumente. Für die tägliche Arbeit spielt das zunächst keine Rolle. Werden diese Informationen später im Kontext einer Copilot-Anfrage relevant, können die weiterhin vorhandenen Rechte jedoch dazu führen, dass Inhalte zugänglich werden, die der Mitarbeiter für seine neue Rolle nicht mehr benötigt.

Vor einem breiten Copilot-Rollout sollte Permission Governance deshalb fester Bestandteil der Sicherheitsplanung sein. Nach dem Least-Privilege-Prinzip sollten Anwender nur die Zugriffe besitzen, die sie für ihre aktuelle Aufgabe benötigen. IT-Verantwortliche sollten dafür Transparenz schaffen: Welche Benutzer und Gruppen können auf sensible Bereiche zugreifen? Welche Rechte werden über Gruppenstrukturen vererbt? Wo bestehen externe Freigaben oder organisationsweit verfügbare Sharing Links? Und welche Zugriffe sind aus fachlicher Sicht überhaupt noch erforderlich?

Ein einmaliger Berechtigungscheck reicht jedoch nicht aus. Rollen, Teams und Projekte verändern sich kontinuierlich. Regelmäßige Permission Audits, definierte Richtlinien sowie nachvollziehbare Prozesse für Rollenwechsel, Offboarding und externe Freigaben helfen dabei, überflüssige Zugriffsrechte frühzeitig zu erkennen.

Die Einführung von Copilot ist damit auch eine Chance für bessere Data Governance. Unternehmen, die ihre Berechtigungen transparent machen, überflüssige Rechte reduzieren und Permission Governance als kontinuierlichen Prozess etablieren, schaffen nicht nur eine bessere Grundlage für den sicheren Einsatz von KI. Sie reduzieren gleichzeitig ein Sicherheitsrisiko, das in vielen Microsoft-365-Umgebungen bereits lange vor Copilot existierte.

Für Unternehmen, die diese Permission Governance systematisch umsetzen möchten, bietet **Hornetsecurity by Proofpoint** mit dem **365 Permission Manager** eine zentrale Lösung für die Verwaltung und Überwachung von Berechtigungen in Microsoft 365. IT-Verantwortliche können Richtlinien für SharePoint, Teams und OneDrive definieren, kritische Freigaben und Richtlinienverstöße erkennen sowie Berechtigungen mithilfe von Quick und Bulk Actions effizient korrigieren. So lässt sich die Transparenz über bestehende Zugriffe erhöhen und das Risiko unnötiger oder unautorisierter interner und externer Freigaben reduzieren – eine wichtige Voraussetzung, um Microsoft 365 und Copilot auf einer kontrollierten Berechtigungsstruktur zu betreiben.