

Teams und Copilot erfordern Firewall-Updates

Microsoft zieht um. Nicht das Büro in Redmond, sondern die Adressen, unter denen deine Leute jeden Tag Teams und Copilot im Browser aufrufen. Wer seine Firewall nicht mitnimmt, erlebt das, was Admins am meisten lieben: einen weißen Bildschirm und eine Ticket-Lawine um 8:01 Uhr.

Executive Summary

Kurz und schmerzlos, wie eine gute Kündigung: Microsoft leitet die Web-Version von Teams von `teams.microsoft.com` auf `teams.cloud.microsoft` um. Parallel landet, wer Microsoft 365 Copilot Chat unter `m365.cloud.microsoft` öffnet, künftig auf `copilot.cloud.microsoft`. Beides passiert automatisch. Niemand fragt dich. Und beides funktioniert nur, wenn deine Firewalls, Proxys, Secure Web Gateways und SSE-Plattformen die komplette Domäne `*.cloud.microsoft` durchlassen.

Der Teams-Umzug sollte bis 30. September 2026 für alle Unternehmens-Tenants durch sein. Für Copilot lief die erste Welle Anfang September, die zweite folgt im Oktober beziehungsweise Anfang November. Für Teams gibt es noch eine Notbremse bis 31. Dezember 2026, danach ist Schluss. Ab 1. Januar 2027 kannst du den Redirect nicht mehr abschalten. Wer heute noch nicht getestet hat, sollte das in den nächsten zwei Wochen mit einer Pilotgruppe nachholen, statt im Januar mit dem Vorstand.

i Fakten: Die zwei Message-Center-Meldungen, die du kennen musst

MC1465764 (1. September 2026): Teams-Webclient wird auf `teams.cloud.microsoft` umgeleitet. Ausnahme nur per Admin-Schalter bis 31.12.2026.

MC1462915 (27. August 2026, zuletzt aktualisiert am 8. Oktober): Copilot Chat zieht von `m365.cloud.microsoft` nach `copilot.cloud.microsoft`. Teilweise Freigaben werden ausdrücklich nicht unterstützt.

Gemeinsamer Nenner: `*.cloud.microsoft` muss erreichbar sein, und zwar vollständig.

Worum geht es im Detail?

Ein bisschen Hintergrund, damit du verstehst, warum Microsoft das überhaupt macht. Über die Jahre hat sich ein Zoo aus Domänen angesammelt: `office.com`, `microsoft.com`, `live.com`, `sharepoint.com`, `office365.com`, dazu Hunderte Subdomänen. Für jede Firewall-Regel ein eigenes Haustier, das gefüttert werden will. Seit 2023 baut Microsoft deshalb die eigene Top-Level-Domain `.microsoft` als zentrales Zuhause für authentifizierte Microsoft-365-Oberflächen auf. `cloud.microsoft` steht seit April 2023 in der offiziellen Netzwerk-Dokumentation. Wer die damals sauber übernommen hat, darf sich jetzt zurücklehnen. Alle anderen haben drei Jahre Vorwarnzeit verschlafen, was im Konzernalltag allerdings eher als normale Reaktionsgeschwindigkeit gilt.

Der Vorteil für Microsoft liegt auf der Hand: Eine eigene TLD gehört niemandem sonst. Kein Phishing-Kollege kann sich [irgendwas.cloud.microsoft](#) registrieren, was bei [.com](#) leider ein Volkssport ist. Für dich bedeutet das langfristig weniger Ausnahmen in der Firewall und eine klarere Antwort auf die Helpdesk-Frage, ob eine Adresse echt ist. Kurzfristig bedeutet es: Regeln anpassen, sonst brennt die Hütte.

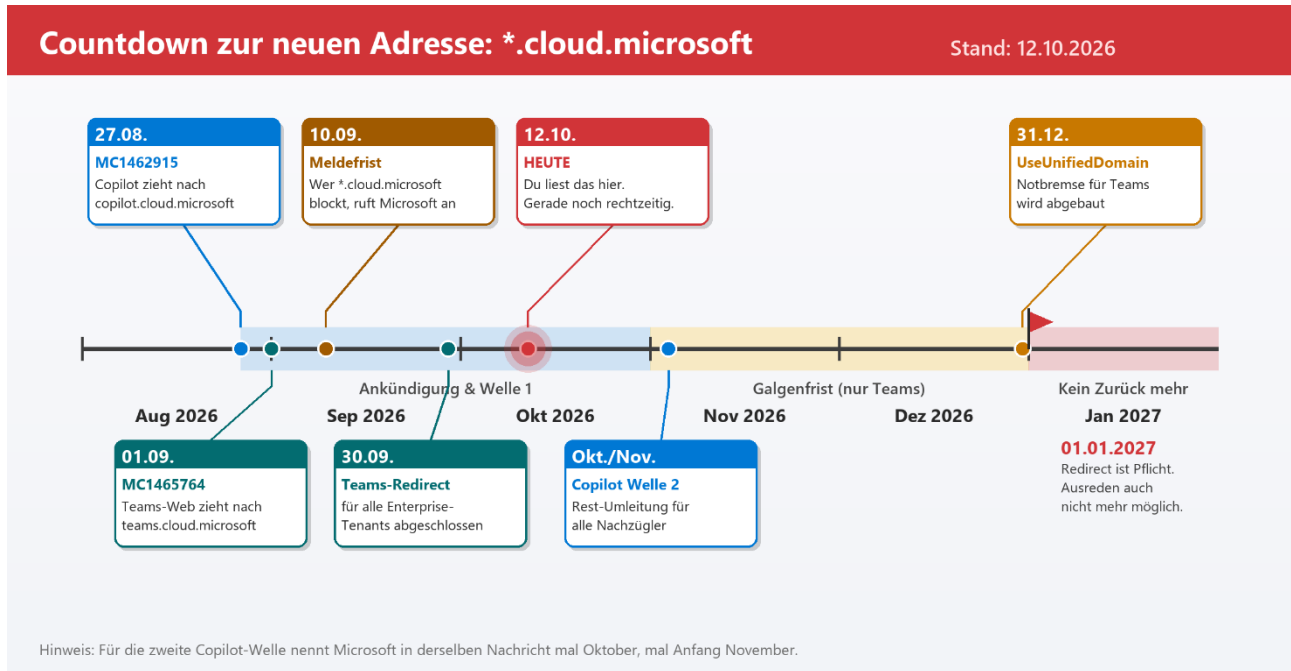
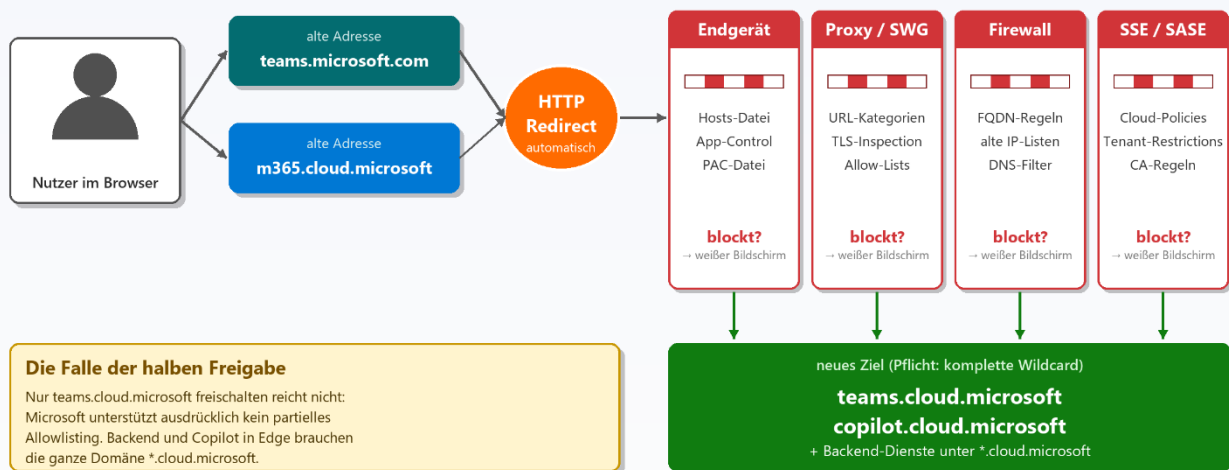


Abbildung 1: Der Zeitplan für Teams und Copilot. Heute ist der 12. Oktober, die Uhr läuft.

Dienst	Alte Adresse	Neue Adresse	Deadline	Notausgang
Teams (Web)	teams.microsoft.com	teams.cloud.microsoft	30.09.2026 Redirect, ab 01.01.2027 Pflicht	UseUnifiedDomain = Disabled bis 31.12.2026
Copilot Chat (Web, Desktop, Edge)	m365.cloud.microsoft	copilot.cloud.microsoft	Welle 1 Anfang Sept., Welle 2 Okt./Nov. 2026	Nur über den Microsoft-Ansprechpartner
Backend-Dienste	diverse	*.cloud.microsoft	sofort	keiner
Teams privat	teams.live.com	unverändert	–	nicht nötig

Technisch ist das Ganze ein simpler HTTP-Redirect. Deine Nutzer klicken auf ein altes Lesezeichen, der Browser bekommt eine Umleitung und landet auf der neuen Adresse. Die Features bleiben gleich, die Oberfläche bleibt gleich, nur die Adresszeile endet plötzlich auf [.microsoft](#). Klingt harmlos. Ist es auch, solange zwischen Browser und Microsoft niemand sitzt, der sich querstellt. Und genau da sitzen in jedem Unternehmen mindestens vier Kandidaten: Endgerät, Proxy, Firewall und die schicke SASE-Plattform, die letztes Jahr für viel Geld eingekauft wurde.

Wo der Redirect stirbt: der Weg vom Klick bis *.cloud.microsoft



Sonderfall: `teams.cloud.microsoft.com` (mit `.com`) gibt es nicht. Wer das tippt, bekommt einen Fehler, keine Umleitung.
 Notausgang für Teams-Web bis 31.12.2026: `Set-CsTeamsClientConfiguration -UseUnifiedDomain Disabled`
 Notausgang für Copilot: keiner. Nur das Gespräch mit dem Microsoft-Ansprechpartner.

Abbildung 2: Vier Kontrollpunkte, vier Gelegenheiten, den Redirect sterben zu lassen.

⚠ Warnung: Halbe Freigaben sind ganze Ausfälle

Microsoft schreibt es in MC1462915 unmissverständlich: Partielles Allowlisting wird nicht unterstützt. Wer nur `teams.cloud.microsoft` und `copilot.cloud.microsoft` freischaltet, weil die Security-Abteilung Wildcards grundsätzlich hasst, bekommt eine halbe App. Backend-Dienste und Copilot in Edge brauchen den ganzen Namensraum `*.cloud.microsoft`. Dazu gehören laut Endpoint-Liste auch `*.static.microsoft` für CDN-Inhalte auf TCP und UDP 443.

Zur Teams-Seite gehört noch ein Detail, das gern übersehen wird: eigene Web-Apps. Wenn deine Entwickler eine Teams-App gebaut haben, die mit einem alten Teams-JavaScript-SDK arbeitet oder in Content-Security-Policy, X-Frame-Options oder Authentifizierungs-Redirects fest `teams.microsoft.com` hinterlegt hat, rendert die nach dem Umzug möglicherweise nicht mehr. Das ist dann kein Firewall-Problem, sondern ein Code-Problem, und landet trotzdem beim Netzwerk-Team, weil die Nutzer "Teams geht nicht" ins Ticket schreiben.

Was sind Chancen? Was sind Risiken?

Fangen wir mit dem Positiven an, das ist schneller erledigt. Die Konsolidierung auf eine einzige, Microsoft-exklusive Domäne ist aus Sicherheitssicht eigentlich ein Geschenk. Du kannst Regeln aufräumen, die seit 2017 niemand mehr verstanden hat, und deinen Nutzern endlich eine einfache Regel beibringen: Was auf `.microsoft` endet, gehört Microsoft. Gleichzeitig ist der Umzug ein hervorragender Vorwand, mal nachzusehen, ob die TLS-Inspection auf dem Proxy für Microsoft-365-Verkehr wirklich abgeschaltet ist, wie es Microsoft seit Jahren empfiehlt.

Chance	Risiko
Weniger Domänen, weniger Regeln, weniger Pflegeaufwand	Ausfall von Teams-Web und Copilot, wenn <code>*.cloud.microsoft</code> blockiert ist
Eigene TLD erschwert Phishing mit Lookalike-Domains	Halbe Freigaben führen zu halbfunktionalen Apps und schwer erklärbaren Fehlern

Chance	Risiko
Anlass für ein Aufräumen alter Proxy- und Firewall-Regeln	Eigene Teams-Web-Apps mit altem SDK oder starrer CSP brechen
Tenant Restrictions v2 ersetzt pauschale Domain-Sperren sauber	Wer Copilot per Domain-Block für Privatkonten sperrt, sperrt jetzt auch das Firmen-Copilot
Bessere Dokumentation und Helpdesk-Wissen	Widersprüchliche Termine in den Microsoft-Meldungen erschweren die Planung

Jetzt zu den Risiken, und da wird es schwarz-humorig. Das größte Risiko ist nicht technischer, sondern organisatorischer Natur. Die Firewall gehört dem Netzwerk-Team, der Proxy der Security, die SASE-Plattform einem externen Dienstleister, der Teams-Tenant dem Modern-Workplace-Team und die Teams-App einer Agentur, die es seit 2024 nicht mehr gibt. Jeder dieser Beteiligten wird dir im Ernstfall glaubhaft versichern, dass es an ihm nicht liegt. Meistens stimmt das sogar, und trotzdem geht nichts.

★ Wichtig: Die Privatkonto-Falle

Manche Unternehmen haben `copilot.cloud.microsoft` bewusst gesperrt, damit niemand mit seinem privaten Microsoft-Konto Firmendaten in Copilot kippt. Gut gemeint, nur sperrst du damit ab sofort auch das lizenzierte Firmen-Copilot. Microsoft empfiehlt stattdessen **Tenant Restrictions v2** in Entra ID: Privatkonten blockieren, Dienst-URL offen lassen. Bei 30 Euro Copilot-Lizenz pro Kopf und Monat ist eine Firewall-Regel, die das Produkt abschaltet, eine ziemlich teure Form von Datenschutz.

Ein Praxisbeispiel, wie es in den letzten Wochen tatsächlich gelaufen ist: Ein Mittelständler aus dem Maschinenbau, rund 1.200 Arbeitsplätze, hatte auf seinem Proxy eine Kategorie-Sperre für "neu registrierte Domains und unbekannte TLDs". Klingt vernünftig, hat jahrelang Malware ferngehalten. Dummerweise stufte der Hersteller des Proxys `.microsoft` intern als exotisch ein. Ergebnis: Am Morgen nach der Umleitung saß der komplette Vertrieb vor einem leeren Teams-Fenster im Browser. Der Desktop-Client lief, also schob die IT das zwei Tage lang auf die Browser. Gefunden hat den Fehler am Ende ein Werkstudent, der in der Browser-Konsole nachgesehen hat. Die Moral: Lies die Konsole, bevor du die Geschäftsführung informierst.

Zweites Beispiel, diesmal aus dem Finanzsektor: Dort hatte das Netzwerk-Team Wildcards per Policy verboten und stattdessen über 300 einzelne FQDNs für Microsoft 365 gepflegt, inklusive Excel-Liste mit Änderungshistorie. Respekt für die Disziplin. Nur: Copilot in Edge rief Backend-Hosts unter `*.cloud.microsoft` auf, die in keiner Liste standen. Die Copilot-Seitenleiste blieb leer, das Board-Mitglied, das gerade seine erste Copilot-Demo zeigen wollte, nicht. Die Wildcard-Policy hat jetzt eine dokumentierte Ausnahme.

Und warum trifft es ausgerechnet die vorsichtigen Unternehmen am härtesten? Weil gute Sicherheitsarchitektur oft aus Misstrauen gegenüber allem Neuen besteht. Eine neue Top-Level-Domain, die plötzlich geschäftskritisch wird, passt in kein Raster, das 2019 jemand in einem Workshop entworfen hat. Viele Secure Web Gateways bewerten Domänen nach Alter, Reputation und Kategorie. Eine Microsoft-TLD ist zwar weder jung noch verdächtig, landet aber je nach Hersteller und Update-Stand in einer Schublade wie "Sonstiges" oder "Unkategorisiert". Und Unkategorisiertes wird in vielen Häusern traditionell erschossen und erst danach befragt.

Dazu kommt TLS-Inspection. Microsoft rät seit Jahren davon ab, Microsoft-365-Verkehr aufzubrechen, weil das Latenz kostet, Zertifikatsprüfungen stört und bei Echtzeit-Medien wie

Teams-Anrufen schlicht zu Aussetzern führt. Wer bisher eine sauber gepflegte Ausnahmeliste für Microsoft-Domänen hatte, muss `*.cloud.microsoft` und `*.static.microsoft` dort ebenfalls eintragen. Sonst funktioniert zwar die Verbindung, aber du baust dir einen hausgemachten Flaschenhals, über den sich hinterher alle beschweren, ohne zu wissen, woran es liegt.

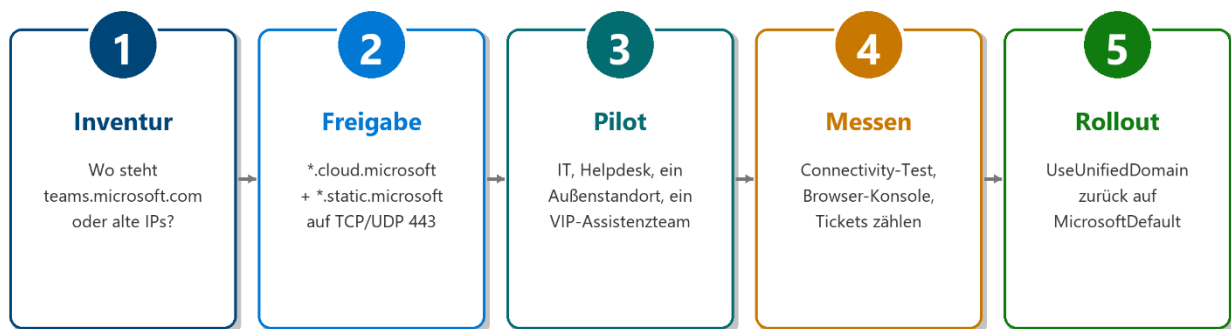
i Fakten: Warum gerade jetzt?

`cloud.microsoft` ist seit April 2023 Teil der offiziellen Netzwerk-Empfehlungen. Die Teams-Umleitung lief schon seit Monaten in kontrollierten Stufen, MC1465764 setzt jetzt den Schlusspunkt. Copilot wurde im August dazugepackt, weil Microsoft die Einstiegsadresse für Copilot Chat auf `copilot.cloud.microsoft` vereinheitlicht.

Was müssen wir jetzt schon vorbereiten?

Die gute Nachricht: Für Teams hast du noch bis Silvester Zeit, die Notbremse zu ziehen und sauber nachzuarbeiten. Die schlechte: Für Copilot gibt es keinen Schalter, nur das Gespräch mit deinem Microsoft-Ansprechpartner, und die Frist dafür war eigentlich schon am 10. September. Also los, und zwar strukturiert statt hektisch.

Pilotgruppe in fünf Schritten: erst testen, dann umschalten



Faustregel: Jeder Schritt bekommt einen Namen, ein Datum und jemanden, der dafür den Kopf hinhält.

Abbildung 3: Der Pilotfahrplan. Langweilig, aber genau deshalb funktioniert er.

- **Inventur:** Durchsuche Firewall-Regeln, PAC-Dateien, Proxy-Kategorien, SSE-Policies, Conditional-Access-Regeln und App-Control-Richtlinien nach `teams.microsoft.com`, `m365.cloud.microsoft` und alten IP-Listen.
- **Freigabe:** Erlaube `*.cloud.microsoft` vollständig, plus `*.static.microsoft`, jeweils TCP und UDP 443. Gleiche alles mit der aktuellen Microsoft-365-Endpoint-Liste ab, nicht mit dem PDF von 2021 aus dem Teams-Kanal.
- **Pilotgruppe:** Nimm IT, Helpdesk, einen Außenstandort mit eigenem Internet-Breakout und ein Assistenzteam der Geschäftsführung. Wer bei denen nichts kaputt macht, hat den Härtestest bestanden.
- **Messen:** Nutze den Connectivity-Test unter `connectivity.m365.cloud.microsoft/copilot`, schau in die Browser-Konsole und zähle die Tickets der Pilotgruppe.
- **Helpdesk briefen:** `teams.cloud.microsoft` ist echt, `teams.cloud.microsoft.com` ist ein Tippfehler. Das muss jeder im First Level aufsagen können.

- **Dokumentation anpassen:** Intranet-Links, Onboarding-Unterlagen und Schulungsvideos aktualisieren. Alte Links funktionieren zwar weiter, aber die Screenshots lügen dann.

✓ Tipp: So prüfst und steuerst du den Teams-Redirect per PowerShell

Aktuellen Stand lesen: `Get-CsTeamsClientConfiguration | select Identity,UseUnifiedDomain | fl`

Notbremse ziehen: `Set-CsTeamsClientConfiguration -Identity Global -UseUnifiedDomain Disabled`

Zurück auf Microsoft-Standard: `Set-CsTeamsClientConfiguration -Identity Global -UseUnifiedDomain MicrosoftDefault`

Die Notbremse ist ein Pflaster, kein Gips. Ab 1. Januar 2027 ist sie weg, egal ob deine Wunde verheilt ist.

Wer	Was	Bis wann
Netzwerk / Firewall	<code>*.cloud.microsoft</code> und <code>*.static.microsoft</code> freigeben, IP-basierte Altregeln prüfen	sofort
Security / Proxy / SSE	Kategorie-Filter, TLS-Inspection und Tenant Restrictions v2 prüfen	Ende Oktober
Modern Workplace	<code>UseUnifiedDomain</code> prüfen, Pilotgruppe steuern, Connectivity-Test fahren	Ende Oktober
App-Entwicklung	Teams-Web-Apps unter neuer Domain testen, SDK und CSP aktualisieren	Ende November
Helpdesk / Kommunikation	Skript für First Level, Intranet-Links, Nutzerinfo	vor Rollout
Projektleitung	Notbremse wieder lösen, Abnahme dokumentieren	spätestens 15.12.2026

⚠ Warnung: Plane nicht bis zum 31. Dezember

Wer die Notbremse am 30. Dezember lösen will, testet zwischen Weihnachtsfeier-Kater und Urlaubssperre. Setze dir den 15. Dezember als echte Frist. Der 31. ist der Tag, an dem du nur noch zusehen kannst.

Häufig gestellte Fragen

Welche Domänen muss ich für Teams und Copilot in der Firewall freigeben?

Du brauchst die komplette Domäne `*.cloud.microsoft`, ergänzt um `*.static.microsoft` für statische Inhalte, jeweils auf TCP und UDP 443. Microsoft unterstützt ausdrücklich keine teilweise Freigabe einzelner Hosts wie nur `teams.cloud.microsoft` oder `copilot.cloud.microsoft`.

Kann ich die Umleitung von Teams auf teams.cloud.microsoft verhindern?

Nur vorübergehend: Mit Set-CsTeamsClientConfiguration und dem Wert UseUnifiedDomain Disabled bleibt der Teams-Webclient bis 31. Dezember 2026 auf teams.microsoft.com. Ab 1. Januar 2027 ist die Umleitung verpflichtend und lässt sich nicht mehr abschalten.

Funktionieren alte Lesezeichen auf teams.microsoft.com weiterhin?

Ja, bestehende Links und Lesezeichen werden automatisch auf die neue Adresse weitergeleitet. Voraussetzung ist, dass das Ziel teams.cloud.microsoft im Netzwerk erreichbar ist, sonst endet die Weiterleitung im Fehler.

Wie verhindere ich private Microsoft-Konten in Copilot, ohne die Copilot-Domäne zu sperren?

Nutze Tenant Restrictions v2 in Microsoft Entra ID, um Anmeldungen mit privaten Microsoft-Konten zu blockieren. So bleibt copilot.cloud.microsoft für die lizenzierten Firmenkonten erreichbar.

Ist der Teams-Desktop-Client von der Domänenumstellung betroffen?

Die Umleitung betrifft den Teams-Webclient im Browser, der Desktop-Client gilt laut Microsoft sogar als Ausweichlösung bei Web-Problemen. Backend-Dienste nutzen aber ebenfalls *.cloud.microsoft, deshalb solltest du die Freigabe trotzdem vollständig umsetzen.