

TEAMS & TELEFONIE

Teams: Identitätsschutz zeigt Warnungen bei möglicher Identitätsfälschung in Besprechungen

Executive Summary

Freitag, 16:40 Uhr. In der Buchhaltung ploppt eine Teams-Einladung auf: „Kurze Abstimmung, streng vertraulich“, Organisator ist der Geschäftsführer. In der Besprechung ist seine Kamera aus, das WLAN im Hotel sei mies, aber die Stimme passt, und er braucht bis Büroschluss eine Anzahlung für eine Übernahme, von der noch niemand wissen darf. Wenn du jetzt denkst, darauf fällt bei uns keiner rein: Genau das hat jede Firma gedacht, die schon einmal draufgefallen ist.

Laut Microsoft-Ankündigung MC1530613 bekommt Teams dafür einen **Identitätsschutz für Besprechungen**. Erkennt Teams einen möglichen Identitätsbetrug, zeigt es Warnungen und Risikohinweise an, und zwar für verdächtige Teilnehmer ebenso wie für verdächtige Organisatoren, vor dem Beitritt und während der Besprechung. Der weltweite Rollout beginnt Mitte Dezember 2026 und soll Ende Dezember abgeschlossen sein. Administratoren müssen nichts einschalten, sollen die Neuerung aber kennen und der Belegschaft und dem Security-Team erklären.

Meine Einordnung: kein Feuerwehreinsatz, aber deutlich mehr als Kosmetik. Microsoft schließt damit die letzte große Lücke in einer Reihe, die 2025 mit Warnungen im Chat begann und 2026 bei den Anrufen weiterging. Die eigentliche Arbeit liegt nicht in der Technik, sondern in der Kommunikation. Denn eine Warnung, die niemand versteht, ist nur ein weiteres Fenster, das man wegklickt. Und dass der Rollout ausgerechnet in die Weihnachtswochen fällt, in denen Vertretungen, Jahresabschlusszahlungen und halb leere Büros Betrügern ohnehin den roten Teppich ausrollen, ist entweder Ironie oder Absicht.

Fakten: Das Wichtigste auf einen Blick

- **Was:** Warnungen und Risikohinweise bei möglicher Identitätsfälschung in Teams-Besprechungen, für Teilnehmer und Organisatoren.
- **Wann:** Rollout weltweit von Mitte bis Ende Dezember 2026; die Meldung läuft bis zum 28.02.2027.
- **Wo:** Laut Roadmap-Eintrag 573157 in Teams für Windows, Mac, Web, iOS und Android, in der weltweiten Standard-Cloud.
- **Admin-Aufwand:** Laut Microsoft keiner. Ob es einen Schalter gibt, ist nicht dokumentiert.
- **Priorität:** Mittel bis hoch. Keine Frist, aber direkte Sicherheitsfolgen und viel Erklärungsbedarf.

Worum geht es im Detail?

Zum Hintergrund: Teams ist längst kein interner Plauderkanal mehr, sondern ein Einfallstor. Der externe Zugriff ist ab Werk für alle Domänen offen, und jeder, der einen Microsoft-365-Mandanten registriert, kann diesem einen beliebigen Anzeigenamen geben. Microsoft Threat Intelligence hat

das mehrfach dokumentiert: 2023 nutzte die russische Gruppe Midnight Blizzard frisch umbenannte Mandanten, die sich als Sicherheits- oder Identitätsteam ausgaben, um per Teams-Chat an Anmeldecodes zu kommen. 2024 überflutete Storm-1811 Postfächer mit Spam, rief dann per Teams als angeblicher Helpdesk an, ließ sich per Fernwartung aufschalten und legte den Weg für Ransomware frei. Laut Microsoft Digital Defense Report 2025 beginnen 28 Prozent der Einbrüche mit Phishing und Social Engineering, und Angreifer bleiben im Schnitt 58 Tage unentdeckt im Netz. Fast zwei Monate, in denen jemand in deinem Netz herumspaziert, ohne dass es auffällt, und das ganz ohne Firmenausweis.

Besprechungen sind dabei die Königsdisziplin des Betrugs, weil sie das stärkste Vertrauenssignal liefern, das wir kennen: ein Gesicht und eine Stimme. Den bekanntesten Fall erlebte Anfang 2024 die Hongkonger Niederlassung des Ingenieurkonzerns Arup. Ein Mitarbeiter überwies rund 25 Millionen US-Dollar, nachdem er in einer Videokonferenz mit dem vermeintlichen Finanzvorstand und mehreren Kollegen gesessen hatte. Alle anderen Teilnehmer waren Deepfakes. Er war, wenn man so will, der einzige Mensch in seiner eigenen Besprechung.

Was ändert sich konkret? Teams bewertet künftig, ob ein Teilnehmer oder ein Organisator einer Besprechung möglicherweise nicht der ist, der er zu sein vorgibt, und blendet dann Warnungen und Risikohinweise ein. Microsoft betont, dass es um zusätzlichen Kontext geht: Teams blockiert nicht, Teams warnt. Die Entscheidung, ob du beitreitest, jemanden aus der Lobby zulässt oder die Besprechung verlässt, bleibt beim Menschen. Das ist konsequent, denn ein falsch blockierter Kunde ist im Vertrieb ungefähr so beliebt wie ein echter Betrüger in der Buchhaltung.

Was Microsoft nicht verrät, ist mindestens so interessant. Welche Signale in die Bewertung einfließen, steht weder in der Meldung noch im Roadmap-Eintrag. Naheliegend sind Merkmale wie Anzeigenname gegen Herkunftsmandant, frisch angelegte oder auffällige Mandanten und Ähnlichkeiten zu Namen aus deiner eigenen Organisation. In der Fachpresse ist auch von einer Auswertung der Medienströme die Rede, also von Deepfake-Erkennung; bestätigt ist das nicht. Ebenso offen: ob es eine Admin-Einstellung gibt, wie die Hinweise genau aussehen und ob die Funktion an eine Lizenz gebunden ist. Der Roadmap-Eintrag nannte zunächst November 2026, die Meldung spricht jetzt von Dezember. Den aktuellen Stand findest du im [Microsoft-365-Roadmap-Eintrag 573157](#).

Die neue Funktion steht nicht allein. Microsoft baut den Schutz in Teams seit zwei Jahren Kanal für Kanal aus, und erst im Zusammenspiel ergibt sich ein Bild:

Schutzfunktion	Kanal	Stand	Steuerung durch Admins
Warnung bei Markenimitation	Chat, externer Erstkontakt	verfügbar seit Februar 2025	nicht konfigurierbar
Schutz vor Imitation eigener Domänen	Chat	verfügbar	nicht konfigurierbar
Warnung vor Betrugsanrufen	VoIP-Anruf, externer Erstkontakt	verfügbar seit Mai 2026	standardmäßig aktiv
Bot-Erkennung in der Lobby	Besprechung	verfügbar seit Juni 2026	Organisator entscheidet über Zulassung
Externe Kontakte melden und blockieren	Chat, Anruf	verfügbar seit Juni 2026	Auswertung in den Schutzberichten

Schutzfunktion	Kanal	Stand	Steuerung durch Admins
Identitätsschutz in Besprechungen	Besprechung, Teilnehmer und Organisator	Rollout Dezember 2026	laut Meldung keine Aktion nötig

Wo Teams den Betrüger abfangen kann

Typischer Ablauf eines Identitätsbetrugs über Teams und die Schutzschicht, die an jeder Stufe greift

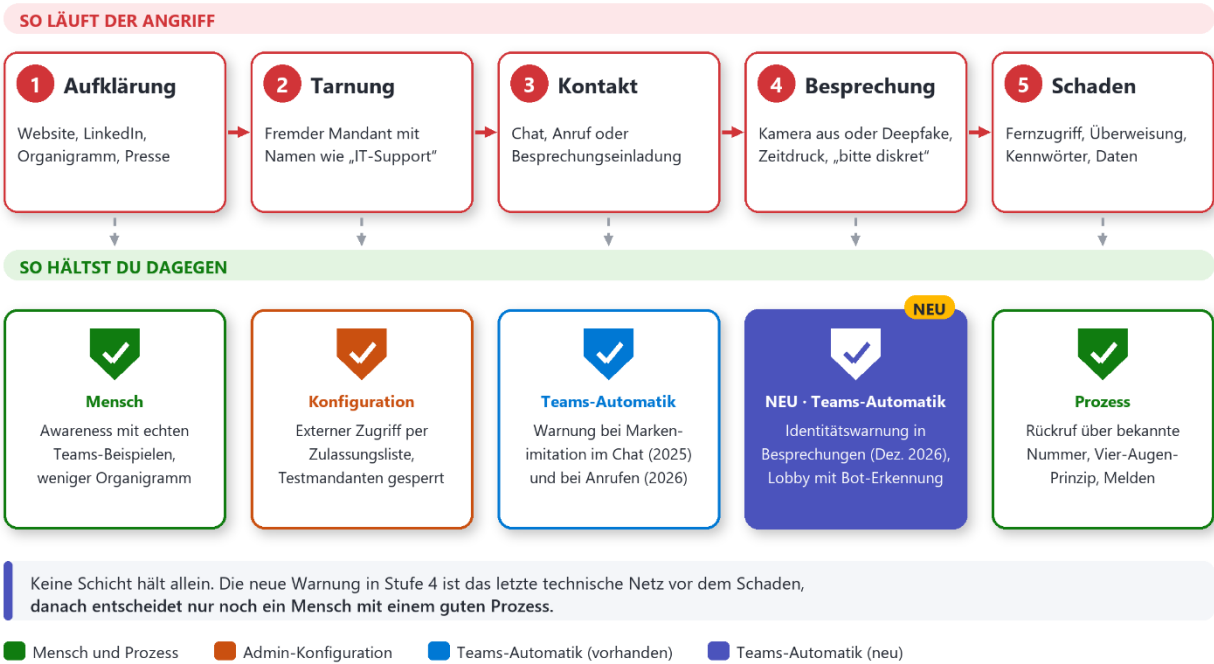


Abbildung 1: Die neue Warnung sitzt an der Stelle, an der Betrug am teuersten wird. Davor und danach brauchst du trotzdem Konfiguration und Prozesse.

Was sind Chancen? Was sind Risiken?

Ein Fall, wie wir ihn in Projekten so oder ähnlich immer wieder sehen: Ein Maschinenbauer in Ostwestfalen, 400 Beschäftigte, Buchhaltung mit drei Leuten. Die Einladung kommt von „Thomas Berger (CEO)“, allerdings aus einem fremden Mandanten, was im Teams-Client nur als unscheinbares „Extern“ neben dem Namen steht. Kamera aus, Zeitdruck, Diskretion, Betrag 380.000 Euro. Gerettet hat das Geld nicht die IT, sondern die Assistenz der Geschäftsführung, die zufällig im Raum stand und sagte: „Der sitzt doch nebenan im Besprechungsraum.“ Genau diesen Zufall will Microsoft durch einen roten Hinweis ersetzen. Gute Idee, denn Zufälle sind als Sicherheitskonzept bekanntlich schlecht skalierbar.

Chancen	Risiken
Warnung genau im Moment der Entscheidung, nicht drei Wochen vorher in der Schulung	Trügerische Sicherheit: Keine Warnung heißt nicht, dass das Gegenüber echt ist
Schützt auch Organisatoren-Fälschung, also die gefälschte Einladung von oben	Fehlalarme bei echten Partnern, etwa einem frisch eingerichteten Mandanten der Steuerkanzlei

Chancen	Risiken
Kein Projekt, keine Konfiguration, kein Budget nach heutigem Stand	Alarmmüdigkeit, wenn Hinweise zu oft und ohne Erklärung erscheinen
Rückenwind für Prozesse wie Rückruf und Vier-Augen-Prinzip	Unbekannte Signale und Trefferquote, also schwer zu bewerten
Bessere Datenlage für das Security-Team über Meldungen und Berichte	Rollout in den Weihnachtswochen mit dünner Besetzung im Helpdesk

Warnung: Die gefährlichste Warnung ist die, die fehlt

Sobald die Belegschaft gelernt hat, dass Teams vor Betrügern warnt, gilt im Umkehrschluss jede Besprechung ohne Warnung als geprüft. Das ist ungefähr so, als würdest du jeden Unbekannten ins Haus lassen, solange der Rauchmelder still ist. Ein gut gemachter Angriff aus einem kompromittierten, echten Partnerkonto löst womöglich gar nichts aus. Schreib deshalb in jede Kommunikation zum Thema in fetten Buchstaben: Die Warnung ist ein Zusatz, kein Freifahrtschein.

Für den **Mittelstand** liegt die größte Chance in der Kombination mit einer sauberen Konfiguration. Wer den externen Zugriff ohnehin auf eine Zulassungsliste bekannter Partnerdomänen beschränkt hat, bekommt mit dem Identitätsschutz eine zweite Linie für den Rest: anonyme Teilnehmer, Gäste und die Fälle, in denen ein Partnerkonto gekapert wurde. Wer alles offen lässt, hat jetzt wenigstens einen Rauchmelder. Feuerfest ist das Haus damit noch nicht.

Öffentliche Auftraggeber haben eine Besonderheit: Bürgersprechstunden und Beteiligungsverfahren leben von anonymen Beitritten. Rechne damit, dass auch harmlose Bürgerinnen und Bürger mal einen Hinweis erzeugen, und gib den Organisatoren eine Linie vor, wie sie damit umgehen. Die Funktion ist laut Roadmap für die weltweite Standard-Cloud angekündigt, also genau dort, wo deutsche Behörden und Kommunen ihre Mandanten betreiben.

Beim **Datenschutz** bleibt die Lage übersichtlich. Die Bewertung von Identitätssignalen ist Teil des Sicherheitsbetriebs von Teams und fällt unter die bestehenden Produktbestimmungen und den Auftragsverarbeitungsvertrag mit Microsoft. Ergänze trotzdem dein Verzeichnis von Verarbeitungstätigkeiten und, falls vorhanden, die Datenschutz-Folgenabschätzung für Teams um einen Satz zur neuen Funktion; spätestens beim nächsten Audit fragt jemand. Spannender ist die **Mitbestimmung**. Die Warnungen selbst überwachen niemanden. Die Melde- und Schutzberichte im Teams Admin Center zeigen aber, wer wann welchen Kontakt gemeldet hat, und damit liegt eine technische Einrichtung im Sinne von § 87 Abs. 1 Nr. 6 BetrVG oder der Personalvertretungsgesetze nahe. Prüfe, ob deine Rahmenvereinbarung zu Teams solche Sicherheitsfunktionen bereits abdeckt, und informiere Betriebs- oder Personalrat vor dem Rollout, nicht danach.

Zur **Lizenz** schweigt die Meldung. Die bisherigen Bausteine für Chat und Anrufe kamen ohne Zusatzkosten, und Microsoft beschreibt die Funktion als Teil von Teams, nicht von Teams Premium. Bis Microsoft etwas anderes dokumentiert, gehe ich davon aus, dass alle Teams-Lizenzen sie erhalten. Wer für besonders vertrauliche Besprechungen mehr will, findet in Teams Premium ergänzende Schutzfunktionen wie erzwungene Lobby-Einstellungen über Vertraulichkeitsbezeichnungen.

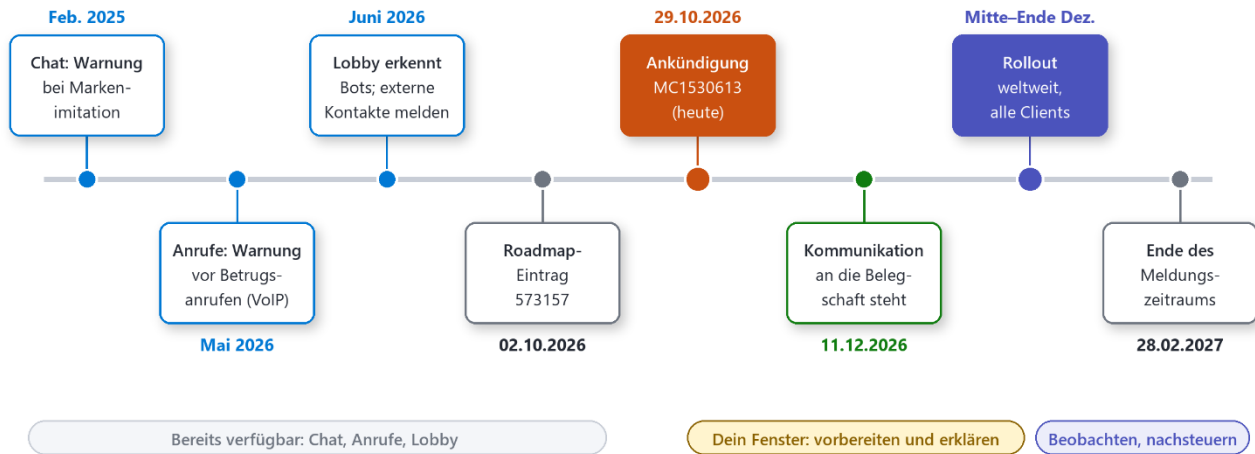
Was müssen wir jetzt schon vorbereiten?

Sechs Wochen bis zum Rollout klingen nach viel Zeit. Abzüglich Jahresendgeschäft, Budgetrunden und Weihnachtsfeier sind es realistisch drei. Der Plan unten ist so geschnitten, dass die Kommunikation vor dem Rollout steht und die Auswertung nach den Feiertagen.

Wann	Was	Wer
Bis 13.11.2026	Externen Zugriff prüfen: Im Teams Admin Center unter Benutzer, Externer Zugriff entscheiden, ob alle Domänen offen bleiben oder eine Zulassungsliste reicht. Kommunikation mit reinen Testmandanten blockiert lassen.	Teams-Admins, Security
Bis 13.11.2026	Lobby-Richtlinien prüfen: Unter Besprechungen, Besprechungsrichtlinien den Wert „Wer kann den Wartebereich umgehen“ mindestens auf Personen der eigenen Organisation und Gäste setzen; anonyme Benutzer dürfen keine Besprechung starten.	Teams-Admins
Bis 27.11.2026	Runbook für Security und Helpdesk: Was tun, wenn jemand eine Warnung meldet? Wer prüft, wer blockiert die Domäne, wer informiert die Betroffenen?	Security, Helpdesk
Bis 27.11.2026	Betriebs- oder Personalrat informieren, Verzeichnis von Verarbeitungstätigkeiten ergänzen.	Datenschutz, HR
Bis 11.12.2026	Belegschaft informieren: kurzer Intranet-Beitrag mit Beispielbild, Hinweis „Warnung ist ein Zusatz“ und Rückrufregel. Organisatoren von Bürger- und Kundenterminen gesondert briefen.	Kommunikation, IT
Mitte bis Ende Dez. 2026	Rollout beobachten, im eigenen Pilotkreis echte Warnungen ansehen, Screenshots für Schulungen sichern, Fehlalarme bei Partnern sammeln.	Teams-Admins, Pilotgruppe
Bis 28.02.2027	Auswertung: Meldungen und Schutzberichte sichten, Fehlalarme mit Partnern klären, Awareness-Schulung um echte Beispiele ergänzen.	Security, IT-Leitung

Vom Chat zur Besprechung: Teams-Schutz in Etappen

Was Microsoft bisher ausgerollt hat, was jetzt kommt und wo dein Zeitfenster liegt



Abstände nicht maßstabsgetreu.

Abbildung 2: Chat und Anrufe sind schon geschützt, die Besprechungen folgen im Dezember. Dein Zeitfenster für die Vorbereitung ist kurz.

Tipp: Die Rückrufregel kostet nichts und schlägt jede KI

Führe eine einfache, verbindliche Regel ein: Jede Zahlung, jede Änderung von Bankdaten und jede Freigabe von Fernzugriff, die in einer Teams-Besprechung angefordert wird, wird über eine bekannte Telefonnummer aus dem Adressbuch bestätigt, nie über eine Nummer aus der Besprechung. Dazu ein Codewort für die Geschäftsführung, das in keinem Organigramm steht. Kein Deepfake der Welt kennt die Durchwahl, die bei euch seit 2009 im Telefonbuch steht.

Wichtig: So erklärst du es der Belegschaft in drei Sätzen

„Ab Dezember warnt Teams, wenn ein Teilnehmer oder Organisator einer Besprechung möglicherweise nicht der ist, der er zu sein vorgibt. Nimm jede Warnung ernst, tritt im Zweifel nicht bei und melde den Fall dem Helpdesk. Und vergiss nicht: Auch ohne Warnung wird keine Zahlung und kein Fernzugriff ohne Rückruf über eine bekannte Nummer freigegeben.“

Für die Feinarbeit an der Konfiguration lohnt sich ein Blick in die Microsoft-Dokumentation, insbesondere in den Learn-Artikel zum [Verwalten externer Besprechungen und Chats](#) und in die Übersicht zum [Verwalten von Lobbyoptionen in Teams](#). Und weil die beste Warnung nichts nützt, wenn das Konto des echten Geschäftsführers mit einem schwachen Kennwort geschützt ist, gehört die Identitätssicherheit in Entra ID gleich mit auf die Liste.

Weiterlesen > [Microsoft Entra pusht Passkeys und verschärft die Identitätssicherheit](#)

Häufig gestellte Fragen

Was zeigt der Identitätsschutz in Teams-Besprechungen an?

Wenn Teams einen möglichen Identitätsbetrug erkennt, blendet es Warnungen und Risikohinweise zu verdächtigen Teilnehmern oder Organisatoren ein, vor dem Beitritt und während der Besprechung. Teams blockiert dabei nicht, die Entscheidung über Beitritt oder Zulassung bleibt beim Nutzer.

Muss der Identitätsschutz für Teams-Besprechungen vom Administrator aktiviert werden?

Laut Microsoft-Ankündigung MC1530613 ist keine Aktion durch Administratoren nötig. Der Rollout läuft weltweit von Mitte bis Ende Dezember 2026, eine Einstellung zum Abschalten ist bisher nicht dokumentiert.

Erkennt Teams damit auch Deepfakes in Videokonferenzen?

Microsoft legt nicht offen, welche Signale ausgewertet werden, und bestätigt eine Deepfake-Erkennung der Bild- und Tonspur nicht ausdrücklich. Verlass dich deshalb nicht darauf und sichere kritische Vorgänge wie Zahlungen zusätzlich durch einen Rückruf über eine bekannte Telefonnummer ab.

Braucht man Teams Premium für den Schutz vor Identitätsfälschung in Besprechungen?

Die Ankündigung nennt keine Lizenzvoraussetzung, und die vergleichbaren Schutzfunktionen für Teams-Chat und Teams-Anrufe sind ohne Zusatzlizenz verfügbar. Teams Premium bietet darüber hinaus ergänzende Funktionen für vertrauliche Besprechungen, etwa erzwungene Lobby-Einstellungen.

Was sollte man tun, wenn Teams vor einem Besprechungsteilnehmer warnt?

Im Zweifel nicht beitreten oder die Person nicht aus der Lobby zulassen, keine Daten, Zugänge oder Zahlungen freigeben und den Fall dem Helpdesk oder Security-Team melden. Die Identität lässt sich am sichersten über einen Rückruf unter einer bekannten Nummer prüfen.