MICROSOFT 365 · STÖRUNG UND RESILIENZ

Der große Microsoft-365-Ausfall: Was bekannt ist und was IT-Chefs daraus lernen sollten

EX1550543 und MO1550821: Warum ein Exchange-Problem halb Microsoft 365 lahmlegte und welche Hausaufgaben jetzt anstehen

Executive Summary

Am Donnerstag, 12. November 2026, ging um 17:17 Uhr MEZ bei Exchange Online das Licht aus. Was Microsoft zunächst als Problem in Nord- und Südamerika meldete, war binnen zwei Stunden eine globale Störung: Downdetector zählte Meldungen aus 74 Ländern, in der Spitze rund 130.000 allein zu Outlook. Und es traf nicht nur die Mail. Teams-Kalender, Copilot, Defender for Office 365, Purview, Intune und Microsoft Graph hingen mit drin, weil sie im Hintergrund auf Exchange Online zugreifen.

Neustarts, Umleitungen und ein Rollback einer Netzwerkänderung brachten in der Nacht nur kurze Atempausen. Erst ein Patch an einer vorgelagerten Authentifizierungs- und Routing-Komponente stabilisierte am Freitagmorgen die Server, seitdem rollt Microsoft ihn Region für Region aus. Eine bestätigte Root Cause gibt es bis Redaktionsschluss nicht; Microsoft schließt einen Angriff aus und hat einen Post-Incident-Report angekündigt.

Die eigentliche Lehre für IT-Chefs hängt aber gar nicht am Root Cause: **Exchange Online ist ein versteckter Single Point of Failure für weite Teile von Microsoft 365**, ausgerechnet auch für die Werkzeuge, mit denen man eine Störung bemerkt, überwacht und kommuniziert. Wer keinen Notfallkanal außerhalb von Microsoft 365 hat, hat jetzt das beste Argument der Welt, das zu ändern.

Worum geht es im Detail?

Der Verlauf in einer Nacht

Schon am Nachmittag gab es ein Vorspiel: Unter TM1550488 meldete Microsoft von 15:45 bis 16:53 Uhr MEZ verzögerte Teams-Chats in Amerika, vorläufige Ursache „resource contention“. Ob das mit dem Hauptvorfall zusammenhängt, ist offen. Um 17:17 Uhr startete EX1550543, um 19:26 Uhr folgte MO1550821 für alle abhängigen Dienste. Gegen 20 Uhr stoppte Microsoft sämtliche Deployments und Konfigurationsänderungen, die klassische Notbremse.

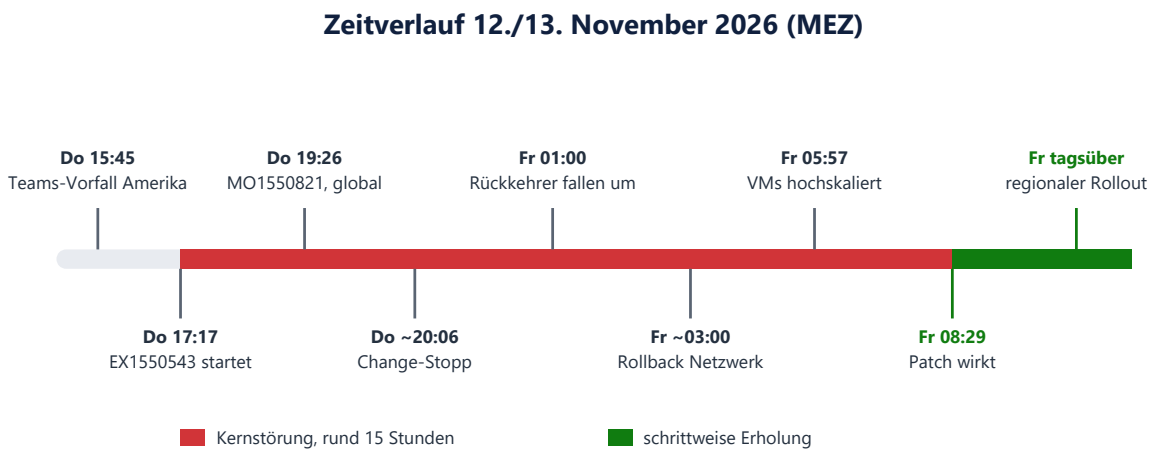


Abbildung 1: Zeitverlauf der Störung (MEZ, gerundet)

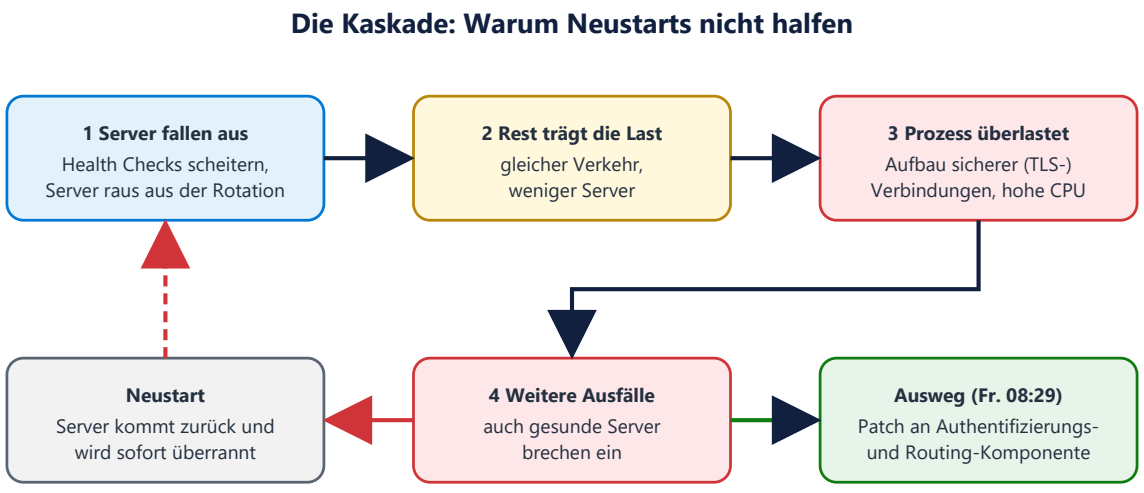
Danach folgte ein zähes Hin und Her: Server wurden mit einer alternativen Health-Check-Methode zurückgeholt, fielen gegen 1 Uhr unter Last wieder um, wurden mit älterer Konfiguration neu aufgebaut, Verkehr wurde gedrosselt und umverteilt. Gegen 4 Uhr räumte Microsoft ein, dass die Maßnahmen nicht wie erwartet greifen, gegen 6 Uhr wurden zusätzliche VMs hochgefahren. Die Wende kam um 8:29 Uhr: Der Patch an der Authentifizierungs- und Routing-Komponente zeigte stabile Server. Parallel verlängerte Microsoft das Zustell-Timeout für E-Mails auf 48 Stunden, damit verzögerte Mails nicht verfallen.

Wie sich Microsofts Erklärung entwickelt hat

Die öffentlichen Erklärungen haben sich im Lauf der Nacht mehrfach verschoben. Das ist bei laufenden Großstörungen normal, zeigt aber auch, wie lange selbst Microsoft im Nebel stand:

Phase	Microsofts Aussage	Was das bedeutet
Do. Abend	Erhöhte Last in mehreren Regionen	Erste Vermutung, noch ohne Ursache
Do. Abend	Last kommt nicht durch mehr Verkehr, sondern durch unerwartet ausgefallene Server, die Health Checks nicht bestehen	Das Problem liegt in der Infrastruktur, nicht beim Kunden
Do. Nacht	Ein Kernprozess auf den Servern ist überlastet, hohe CPU-Last	Neustarts helfen nur kurz
Fr. früh	Der Prozess für den Aufbau sicherer Verbindungen ist überlastet; Rollback einer Netzwerkänderung	Rollback bringt keine nachhaltige Besserung
Fr. Morgen	Patch an vorgelagerter Authentifizierungs- und Routing-Komponente stabilisiert die Server	Erster wirksamer Hebel, regionaler Rollout

Das Muster dahinter ist eine Kaskade: Fallen genug Server aus der Rotation, übernehmen die verbliebenen deren Verkehr, laufen ihrerseits voll und fallen ebenfalls. Jeder neu gestartete Server bekommt sofort die volle Wucht ab und ist nach Minuten wieder weg. Beobachtungen aus der Admin-Community passen ins Bild: Verbindungen zu Outlook-Hosts scheiterten oft schon beim TLS-Handshake, während Anmeldung, Graph-Endpunkte und Teams antworteten. Bestätigt ist das von Microsoft nicht.



Rot: der Teufelskreis der Nacht zum Freitag. Grün: erst die Korrektur vorgelagert brachte Stabilität.
Darstellung auf Basis der Microsoft-Statusmeldungen, Root Cause noch nicht bestätigt.

Abbildung 2: Die Kaskade aus Serverausfall, Überlast und Neustart

Und das „fehlerhafte Update“? Mehrere Medien berichten unter Berufung auf Regierungsstellen, Microsoft gehe von einem fehlerhaften Update bzw. von Einstellungen nach einem Update aus. Auf der offiziellen

Statusseite steht das so nicht. Auch einen Zusammenhang mit dem Patchday zwei Tage zuvor hat Microsoft nicht hergestellt. Bis zum Post-Incident-Report gilt also: plausible Spur, keine bestätigte Ursache.

Warum gleich halb Microsoft 365 betroffen war

Spannender als die Ursache ist die Wirkung. Microsoft hat es selbst so formuliert: Betroffen ist alles, was mit Exchange Online und E-Mail interagiert, was ohne Exchange auskommt, läuft weiter. Diese Abhängigkeiten stehen in keinem Lizenzvertrag und in kaum einer Notfallplanung.

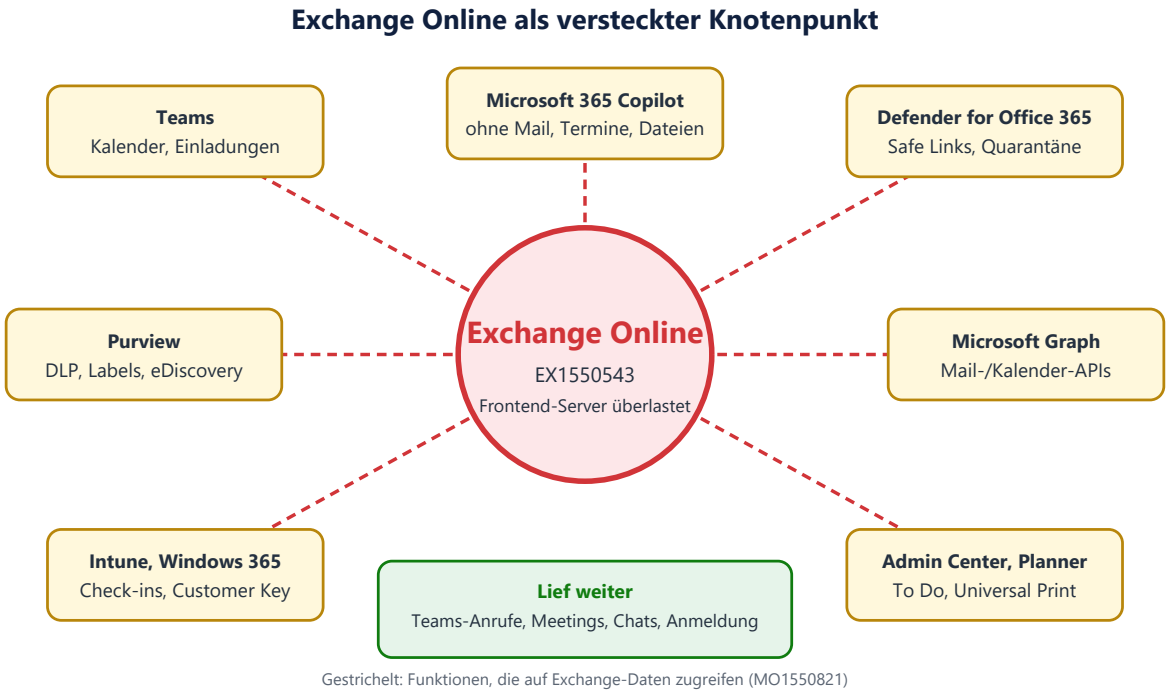


Abbildung 3: Exchange Online als versteckter Knotenpunkt in Microsoft 365

Dienst	Was nicht ging	Was weiterlief
Exchange Online	Postfachzugriff über OWA, Outlook (MAPI), ActiveSync, REST; Zustellung verzögert	Mails wurden laut Microsoft verzögert, nicht verloren
Teams	Termine planen, Einladungen, Events, bestimmte Kanäle anlegen	Anrufe, Meetings, Gruppen- und Kanalchats
Defender for Office 365	Safe Links lösten URLs nicht auf, Quarantäne-Freigaben und Message Trace hakten	Grundschutz der Mail-Pipeline
Purview, Defender XDR	Portalseiten, DLP, Sensitivity Labels, Audit-Suche, eDiscovery teils gestört	Nicht exchangeabhängige Funktionen
Copilot, Graph, Intune, Windows 365	Copilot ohne Mail/Kalender, Graph-Timeouts, Intune-Check-ins, Cloud-PCs mit Customer Key	Grundfunktionen ohne Exchange-Daten

FAKTEN | Die Störung in Zahlen

- Kennungen: **EX1550543** (Exchange Online), **MO1550821** (abhängige Dienste), Vorspiel **TM1550488** (Teams, Amerika)
- Beginn: 12.11.2026, 17:17 Uhr MEZ; Kernstörung rund 15 Stunden, danach regionale Erholung
- Reichweite: Meldungen aus 74 Ländern, Spitze rund 130.000 Outlook-Meldungen auf Downdetector
- Kein Hinweis auf einen Angriff; Post-Incident-Report von Microsoft angekündigt
- Nicht der erste Fall: Ende August (EX1464935) legte eine zentrale Authentifizierungskonfiguration Exchange Online lahm, im Juli ein Fehler in der automatisierten Netzwerkwartung Teile von Microsoft 365 und Azure

Was sind Chancen? Was sind Risiken?

Klingt zynisch, aber ein solcher Ausfall ist für die IT-Leitung auch eine Gelegenheit. Selten hört die Geschäftsführung so aufmerksam zu wie am Tag danach.

Die Risiken

- **Konzentrationsrisiko:** Mail, Kalender, Kollaboration, Security und KI hängen am selben Backend. Ein Problem dort ist kein Mail-Problem, sondern ein Betriebsproblem.
- **Blindflug:** Service-Health-Benachrichtigungen an ein Exchange-Online-Postfach, Monitoring-Alarme über das Exchange-Online-Relay, das Notfallhandbuch auf SharePoint. Genau dann, wenn man es braucht, ist es weg.
- **Sicherheitslücke auf Zeit:** Safe Links lief ins Leere, Quarantäne und Message Trace hakten. Gleichzeitig ist eine solche Störung ein Festmahl für Phishing-Mails und falsche „Microsoft-Support"-Anrufe.
- **Hybrid-Fallstricke:** Lokale Exchange-Server stauen Mails Richtung Exchange Online. Der Standardwert für `MessageExpirationTimeout` liegt bei zwei Tagen, danach gibt es Unzustellbarkeitsberichte.
- **Regulatorik:** NIS2 (Art. 21) verlangt Maßnahmen zur Aufrechterhaltung des Betriebs und zur Sicherheit der Lieferkette. Ob ein Vorfall wie dieser meldepflichtig ist (Art. 23), ist im Einzelfall zu bewerten, dokumentieren muss man ihn so oder so.

Die Chancen

- **Budgetargument:** Notfallkommunikation und Business-Continuity-Planung waren bisher „nice to have". Ab heute haben sie eine Erzählung, die jeder Vorstand versteht.
- **Ehrliche Abhängigkeitsanalyse:** Jetzt lässt sich sauber erheben, welche Prozesse ohne Mail und Kalender tatsächlich stillstanden. Das ist Gold für die nächste Business-Impact-Analyse.
- **Realistische Erwartungen:** 99,9 Prozent Verfügbarkeit heißt rund 43 Minuten Ausfall pro Monat, ganz legal. Wer das intern einmal ausspricht, führt künftig entspanntere Gespräche.

WICHTIG | Cloud-Flucht ist nicht die Antwort

Der Reflex „zurück zum eigenen Exchange" greift zu kurz. Lokale Exchange-Server SE, 2016 und 2019 hatten erst nach den Oktober-Updates eigene, schwere Störungen, und die Patch-, Härtungs- und Betriebslast liegt dann vollständig im Haus. Die richtige Antwort ist Resilienz rund um Microsoft 365: Notfallkanäle, Alarmierung und Dokumentation außerhalb der Plattform.

WARNUNG | Typisierte Praxisanekdote: Der Alarm, der nie ankam

Ein mittelständischer Fertiger, sauber aufgestellt, alles in Microsoft 365. Die Service-Health-Benachrichtigungen gehen ans IT-Sammelpostfach, das Monitoring verschickt Alarme über das Exchange-Online-Relay, das Notfallhandbuch liegt fein versioniert in SharePoint. Am Donnerstagabend erfährt die IT von der Störung nicht durch ihr Monitoring, sondern durch den Vertriebsleiter, der auf dem Privathandy anruft, weil er „seit einer Stunde keine Mails“ hat. Die Telefonliste der Abteilungsleitungen? Steht in Outlook. Kein Einzelfall, sondern das typische Muster, wenn Überwachung und Kommunikation auf demselben Backend laufen wie das, was sie überwachen sollen.

Was müssen wir jetzt schon vorbereiten?

Sofort, solange die Erholung noch läuft, gilt: am Client nichts reparieren. Office neu installieren, Outlook-Profile löschen oder Passwörter zurücksetzen bringt nichts, erzeugt aber nach der Störung zusätzliche Last und Tickets. Auch eigene Änderungen an Transportregeln, Connectoren oder Conditional Access gehören eingefroren, damit sich Fehlerbilder später sauber trennen lassen. Und Safe Links bitte nicht abschalten, nur weil Links gerade nicht aufgehen.

Szenario	Empfehlung	Begründung
Störung läuft noch	Change-Freeze, keine Client-Reparaturen, Belegschaft über einen Nicht-Microsoft-Kanal informieren	Ursache liegt bei Microsoft; jede Bastelei erzeugt Folgeschäden
Exchange-Hybrid im Einsatz	Warteschlangen mit `Get-Queue` prüfen, Ablaufzeit befristet verlängern und danach zurücksetzen	Verhindert Unzustellbarkeitsberichte nach zwei Tagen
Nach der Erholung	Hängengebliebene Mails mit `Get-MessageTraceV2` (Status Pending/Failed) suchen	Verzögerte Zustellung ist kein Verlust, aber nicht immer vollständig
Post-Incident-Report erschienen	Report sichern und intern auswerten	Service Health zeigt nur 30 Tage Historie
Phishing-Welle mit Störungsbezug	Belegschaft aktiv warnen, Support-Rückrufe nur über bekannte Nummern	Angreifer nutzen jede Großstörung als Köder

TIPP | Status abfragen, auch wenn das Admin Center hängt

Das Admin Center war selbst betroffen. Über das Graph-PowerShell-Modul lassen sich beide Vorfälle trotzdem abrufen: `Get-MgServiceAnnouncementIssue -ServiceHealthIssueId EX1550543` liefert Status und Meldungshistorie, den späteren Bericht holt `Get-MgServiceAnnouncementIssueIncidentReport`. Ohne Anmeldung hilft status.cloud.microsoft.

Mittelfristig geht es um die Hausaufgaben, die dieser Ausfall schonungslos aufgedeckt hat. Keine davon ist teuer, aber jede braucht einen Namen und ein Datum:

Was	Wer	Bis wann
Service-Health-Benachrichtigungen zusätzlich an eine Adresse außerhalb von Microsoft 365 leiten	IT-Betrieb	Sofort
Notfallkanal festlegen, der weder an Exchange noch an Teams hängt (SMS-Verteiler, Telefonkette, externes Statusportal)	IT-Leitung mit Kommunikation	Bis Jahresende
Telefonliste und Notfallhandbuch offline bzw. außerhalb von SharePoint vorhalten	IT-Leitung	Bis Jahresende

Was	Wer	Bis wann
Systemalarme über einen zweiten Relay- oder Benachrichtigungsweg versenden	IT-Betrieb	Q1 2027
Interne Aufstellung: betroffene Abteilungen, Dauer, stillstehende Prozesse, funktionierende Ausweichwege	IT-Leitung mit Fachbereichen	In den nächsten zwei Wochen
Abhängigkeiten von Exchange Online inventarisieren (Copilot, Purview, Workflows, Graph-Anwendungen)	Architektur	Q1 2027
Vorfall für NIS2 dokumentieren, Meldepflicht prüfen	ISB mit Datenschutz	Zeitnah

Häufig gestellte Fragen

War das ein Cyberangriff?

Nach allem, was bekannt ist: nein. Microsoft hat ausdrücklich erklärt, es gebe keine Hinweise auf böswillige Aktivitäten. Die Muster aus Serverausfällen, Überlast und erfolglosen Neustarts sprechen für einen technischen Fehler in der eigenen Infrastruktur. Endgültig klären wird das erst der Post-Incident-Report.

Sind E-Mails verloren gegangen?

Microsoft meldet Verzögerungen, keinen Mailverlust. Absendende Server versuchen in der Regel über Tage erneut zuzustellen, und Microsoft hat das eigene Zustell-Timeout auf 48 Stunden verlängert. Wer Exchange Hybrid betreibt, sollte die lokalen Warteschlangen im Blick behalten. Nach der Erholung lohnt ein Blick in den Message Trace auf Nachrichten im Status „Pending“ oder „Failed“. Mails bitte nicht pauschal erneut senden lassen, sonst gibt es Dubletten.

Steht uns eine Gutschrift zu?

Möglicherweise ja, aber erwarte keine Reichtümer. Das SLA sichert 99,9 Prozent monatliche Verfügbarkeit zu. Darunter gibt es 25 Prozent Gutschrift, unter 99 Prozent (mehr als rund 7,2 Stunden) 50 Prozent, unter 95 Prozent 100 Prozent, jeweils nur auf den Preisanteil des betroffenen Dienstes und gerechnet in Benutzerminuten. Die Gutschrift kommt nicht automatisch: Du musst sie per Service Request im Admin Center beantragen, mit Incident-IDs, Zeiträumen und Zahl der Betroffenen, und zwar bis 31.12.2026. Wer über einen CSP-Partner lizenziert, geht über den Partner. Einen Schadensersatz für Betriebsausfall gibt es nicht.

Hätte uns ein eigener Exchange-Server geschützt?

Vor genau diesem Ausfall ja, vor Ausfällen insgesamt nein. Ein lokaler Exchange hat seine eigenen Risiken, wie die Probleme nach den Oktober-Updates gezeigt haben, und dazu kommt der komplette Betriebs- und Sicherheitsaufwand. Sinnvoller ist es, die Kommunikations- und Alarmierungswege, die im Ernstfall gebraucht werden, bewusst außerhalb der Plattform zu halten.

Was machen wir mit dem Post-Incident-Report?

Sichern, lesen, verwerten. Service Health zeigt nur 30 Tage Historie, danach ist der Bericht im Portal weg. Interessant sind vor allem die angekündigten „Defense-in-Depth“-Maßnahmen: Sie zeigen, ob Microsoft die Kaskade strukturell bricht. Für die eigene Dokumentation, etwa gegenüber Prüfern oder im Rahmen von NIS2, ist der Bericht ohnehin ein Pflichtanhang.

Stand: 13.11.2026, 18:30 Uhr. Eine abschließende Ursache hatte Microsoft bis dahin nicht veröffentlicht.