

MICROSOFT 365

Störung bei Global Secure Access: M365-Zugriff in Deutschland stundenlang beeinträchtigt

Du hast einen Sicherheitstunnel gebaut, damit niemand Unbefugtes reinkommt. Am 13. Oktober hat er zuverlässig funktioniert: Es kam auch niemand Befugtes rein.

Executive Summary

Am Dienstag, dem 13. Oktober 2026, konnten Nutzer in Deutschland, die Microsoft 365 über **Global Secure Access (GSA)** erreichen, stundenlang nicht oder nur stockend auf Outlook, Outlook im Web, OneDrive, SharePoint Online, Teams und Windows 365 Cloud PCs zugreifen. Laut finalem Microsoft-Update dauerte die Störung von 07:40 bis 18:31 UTC, also von 09:40 bis 20:31 Uhr deutscher Zeit. Knapp elf Stunden. Ein kompletter Arbeitstag plus Überstunden, nur ohne Arbeit.

Als Ursache nannte Microsoft in den Zwischenmeldungen einen Teil der GSA-Infrastruktur, der unterhalb der akzeptablen Leistungsschwellen lief. Behoben wurde das durch Umleiten des Traffics und gezielte Neustarts. Der einzige offizielle Workaround, nämlich GSA zu deaktivieren, tauchte auf der Statusseite erst um 18:20 UTC auf. Elf Minuten vor dem Ende. Das ist ungefähr so hilfreich wie ein Rettungsring, den man dir zuwirft, während du schon am Strand stehst.

Die eigentliche Lehre steckt aber nicht bei Microsoft, sondern bei dir: Wer GSA sauber gehärtet hat, also Nutzern das Abschalten des Clients verbietet und per Conditional Access ein „Compliant Network“ verlangt, kann genau diesen Workaround gar nicht ausführen, ohne sich selbst auszusperren. Du brauchst deshalb jetzt einen vorbereiteten Notausgang: zentral schaltbar, getestet und mit klarer Entscheidungsbefugnis.

FAKTEN: Die Störung in Zahlen

Datum: Dienstag, 13. Oktober 2026

Zeitraum: 07:40 bis 18:31 UTC (09:40 bis 20:31 Uhr MESZ), 10 Stunden 51 Minuten

Betroffen: Nutzer mit GSA-Zugriff auf Microsoft 365, anfangs in Deutschland und Großbritannien, ab 17:26 UTC nur noch Deutschland

Dienste: Outlook, Outlook im Web, OneDrive, SharePoint Online, Teams, Windows 365 Cloud PCs

Ursache laut Microsoft: Teil der GSA-Infrastruktur unter den akzeptablen Leistungsschwellen

Workaround: GSA deaktivieren, veröffentlicht um 18:20 UTC

Post-Incident-Report: zum Redaktionsschluss nicht veröffentlicht

Worum geht es im Detail?

Was Global Secure Access eigentlich macht

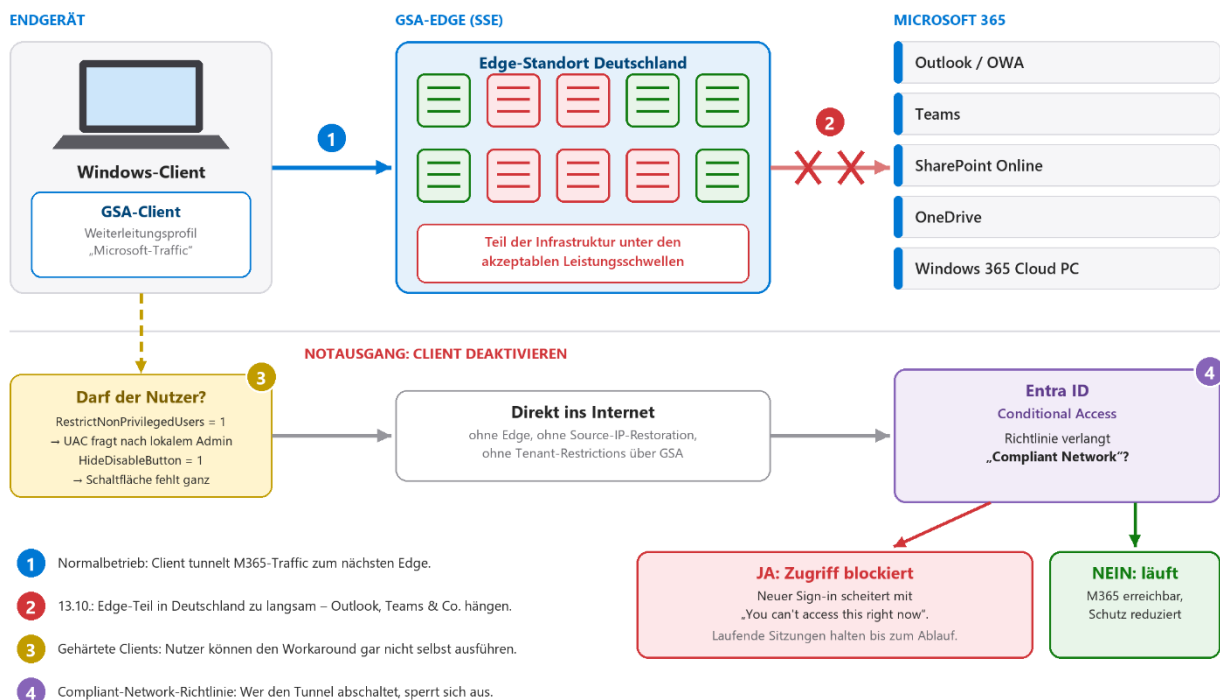
Global Secure Access ist Microsofts Security Service Edge, das Dach über Entra Internet Access und Entra Private Access. Das Prinzip: Ein Client auf dem Gerät fängt definierten Traffic ab und schickt ihn durch einen Tunnel zum nächstgelegenen Microsoft-Edge-Standort. Welcher Traffic das ist, legst du über **Weiterleitungsprofil** fest. Das Microsoft-Traffic-Profil kümmert sich um Exchange Online, SharePoint, OneDrive, Teams und Co. Alles andere geht direkt raus.

Warum macht man das überhaupt, wenn M365 sowieso in der Cloud liegt? Wegen der Extras. Über den Tunnel bekommst du **Universal Tenant Restrictions**, damit niemand Firmendaten in einen privaten Tenant schiebt. Du bekommst **Source-IP-Restoration**, damit Entra trotz Tunnel die echte Absender-IP sieht. Und du bekommst das Schmuckstück: die **Compliant-Network-Prüfung** in Conditional Access. Damit lässt du Anmeldungen nur noch zu, wenn sie durch den GSA-Tunnel deines eigenen Tenants kommen. Gestohlene Tokens, die jemand von irgendwo auf der Welt wiederverwenden will, laufen ins Leere. Ohne lästiges Pflegen von IP-Listen und ohne den Umweg über das Firmen-VPN.

Klingt großartig, und ist es auch. Bis zu dem Tag, an dem der Tunnel selbst lahmt. Dann hängt plötzlich deine komplette Produktivumgebung an einem einzigen Glied, das du weder siehst noch reparieren kannst.

Der Weg deines M365-Traffics – und warum der Notausgang klemmen kann

Oben der Normalbetrieb mit Microsoft-Traffic-Profil, unten der Workaround „GSA deaktivieren“



Fazit: Ein Workaround, den niemand ausführen darf und den die eigene Richtlinie blockiert, ist Deko.

Abbildung 1: Normalbetrieb über den GSA-Edge, der Engpass am 13. Oktober und warum der Workaround in gehärteten Umgebungen klemmt

Was am 13. Oktober passiert ist

Die Chronologie liest sich wie ein Krimi, bei dem der Kommissar erst nach der Mittagspause auftaucht. Die ersten Meldungen nannten 08:00 UTC als Beginn, das finale Update korrigierte auf

07:40 UTC. Betroffen waren zunächst Nutzer in Deutschland und Großbritannien. Die erste dokumentierte Gegenmaßnahme kam um 14:38 UTC: Traffic-Optimierungen, nach denen die Fehler zurückgingen, aber nicht verschwanden. Um 14:59 UTC benannte Microsoft die Ursache und begann, den Traffic von der schwächelnden Infrastruktur wegzuleiten. Um 15:24 UTC war die Umleitung abgeschlossen.

Dann folgte die klassische IT-Therapie: aus- und wieder einschalten. Ab 16:25 UTC startete Microsoft die nun entlasteten Systeme neu, interne Tests zeigten Besserung für einen Teil der Nutzer. Um 17:26 UTC war Großbritannien raus, Deutschland blieb drin. Um 18:20 UTC kam der Workaround, um 18:31 UTC endete die Störung laut Microsoft, und um 18:48 UTC folgte das finale Update mit Bestätigung durch Telemetrie und Kundenrückmeldungen. Bemerkenswert: Die Ursache mit den Leistungsschwellen steht nur in den Zwischenmeldungen, das finale Update wiederholt sie nicht.

13. Oktober 2026: knapp elf Stunden im Nebel

Ablauf der GSA-Störung laut Microsoft-Statusupdates. Oben UTC, darunter deutsche Zeit (MESZ = UTC + 2).

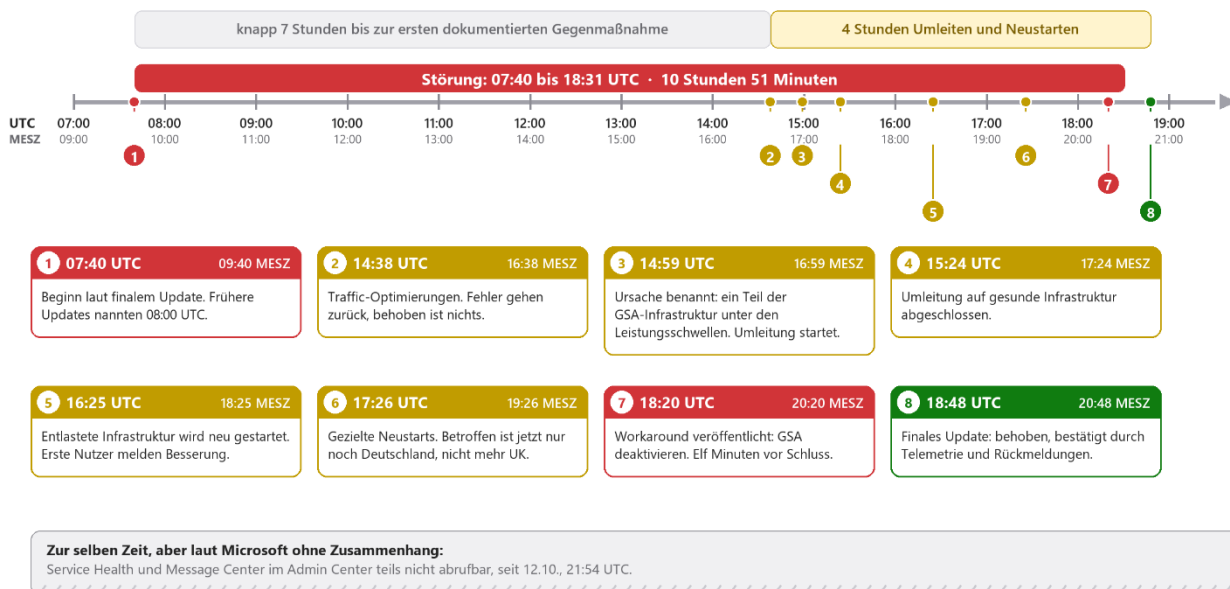


Abbildung 2: Zeitleiste der Störung mit allen Statusupdates in UTC und deutscher Zeit

Und weil schlechte Tage selten allein kommen: Parallel lief ein separater Vorfall, bei dem Admins im Microsoft 365 Admin Center teilweise weder Service-Health-Meldungen noch Message-Center-Beiträge sehen konnten, beginnend am 12. Oktober um 21:54 UTC. Microsoft sagt, das habe nichts mit GSA zu tun. Für dich als Admin fühlte es sich trotzdem an wie ein Brand, bei dem gleichzeitig der Rauchmelder auf stumm steht. Es war übrigens nicht der erste Wackler der letzten Wochen: Am 16. September hatten Nutzer in den USA Zugriffsprobleme, am 5. und 6. Oktober kamen Admins teilweise nicht ins Admin-Portal.

WARNUNG: Die Statusseite ist kein Frühwarnsystem

Der Workaround stand erst nach 10 Stunden 40 Minuten auf der öffentlichen Statusseite. Wer auf Microsoft wartet, bis es „GSA deaktivieren“ sagt, wartet einen ganzen Arbeitstag. Dein Helpdesk merkt das Problem nach fünf Minuten am Telefon. Die Entscheidung über den Notausgang gehört deshalb in dein Haus, nicht nach Redmond.

Was sind Chancen? Was sind Risiken?

Die Risiken

Das größte Risiko ist ein Architekturproblem, das man sich mit besten Absichten selbst baut. Szenario aus einem typischen Mittelständler mit 400 Leuten: Die IT hat GSA vorbildlich eingeführt. Der Disable-Knopf im Client ist per Registry ausgeblendet, RestrictNonPrivilegedUsers steht auf 1, eine Conditional-Access-Richtlinie blockiert alle Anmeldungen außerhalb des Compliant Networks. Der CISO ist stolz, der Auditor zufrieden. Am 13. Oktober um 09:45 Uhr klingelt das Helpdesk-Telefon, um 10:15 Uhr klingelt es ununterbrochen. Und jetzt? Nutzer können den Client nicht abschalten, weil die UAC lokale Admin-Rechte verlangt. Schaltet die IT den Tunnel zentral ab, greift die Compliant-Network-Richtlinie, und neue Anmeldungen scheitern mit „You can't access this right now“. Laufende Sitzungen halten noch bis zum nächsten Token-Refresh, danach ist Schicht. Wer das nicht vorher durchgespielt hat, diskutiert das um 11 Uhr im Krisen-Teams-Call. Ach nein, Teams geht ja nicht.

Das zweite Risiko ist subtiler: die Admins selbst. Wenn deine Admin-Arbeitsplätze ebenfalls über GSA laufen und die Compliant-Network-Richtlinie auch für Admin-Konten gilt, kommst du im Ernstfall womöglich nicht einmal ins Entra Admin Center, um den Tunnel abzuschalten. Microsoft empfiehlt nicht ohne Grund, Notfallzugriffskonten aus solchen Richtlinien auszunehmen. Viele Tenants haben Break-Glass-Konten, aber niemand weiß, wo der Zettel mit dem FIDO2-Schlüssel liegt.

Drittens wird jede Abschaltung zum Sicherheitskompromiss. Ohne Tunnel fallen Tenant Restrictions über GSA weg, und ohne Source-IP-Restoration sehen IP-basierte Named Locations plötzlich Heim- und Hotel-IPs. Wer also den Notausgang öffnet, öffnet auch ein Fenster. Das ist vertretbar, wenn es bewusst passiert, befristet ist und protokolliert wird. Es ist fahrlässig, wenn es um 16 Uhr aus Verzweiflung passiert und drei Wochen lang niemand den Schalter zurücklegt.

Die Chancen

Klingt jetzt so, als solltest du GSA wieder rauswerfen. Solltest du nicht. Die Störung ist der kostenlose Stresstest, für den du sonst einen Workshop hättest bezahlen müssen. Sie zeigt dir, wo deine Zero-Trust-Architektur keine Redundanz hat, und zwar bevor ein Angreifer oder ein noch längerer Ausfall es dir zeigt. Wer jetzt einen Notfallpfad baut, hat danach beides: harte Sicherheitsregeln im Normalbetrieb und einen kontrollierten Ausweg im Störfall. Und du hast endlich ein Argument, mit dem du das Budget für ein vernünftiges Runbook und eine Monitoring-Lösung bekommst, die nicht von Microsofts Statusseite abhängt.

Härtungsmaßnahme	Nutzen im Normalbetrieb	Folge bei GSA-Störung	Notfall-Gegenmittel
Disable-Knopf ausgeblendet (HideDisableButton = 1)	Nutzer umgehen den Tunnel nicht versehentlich	Nutzer können den Workaround nicht selbst ausführen	Zentrale Abschaltung über das Weiterleitungsprofil
RestrictNonPrivilegedUsers = 1	Abschalten nur mit lokalem Admin	UAC-Abfrage, Helpdesk wird zum Flaschenhals	Intune-Remediation oder zentraler Schalter vorbereiten
Conditional Access: Compliant Network	Gestohlene Tokens von außen nutzlos	Ohne Tunnel scheitern neue Anmeldungen	Vorbereitete Notfall-Ausschlussgruppe
Admin-Konten in derselben Richtlinie	Einheitliche Regeln	Admins sperren sich beim Gegensteuern aus	Break-Glass-Konten ausnehmen und testen

Härtungsmaßnahme	Nutzen im Normalbetrieb	Folge bei GSA-Störung	Notfall-Gegenmittel
Source-IP-Restoration plus IP-Standorte	Echte Absender-IP in Entra	Ohne Tunnel andere IPs, andere Richtlinienwirkung	IP-Richtlinien vorab auf Notbetrieb prüfen

Was müssen wir jetzt schon vorbereiten?

Die gute Nachricht: Alles, was du brauchst, gibt es schon. Du musst es nur vor dem nächsten Ausfall zusammenbauen und nicht währenddessen. Der Unterschied ist ungefähr der zwischen Feuerlöscher kaufen und Feuerlöscher bei Amazon bestellen, während die Küche brennt.

Notfall-Runbook: GSA hakt, M365 steht

Vier Entscheidungen, die du heute triffst, damit du sie beim nächsten Mal nicht um 10 Uhr morgens triffst

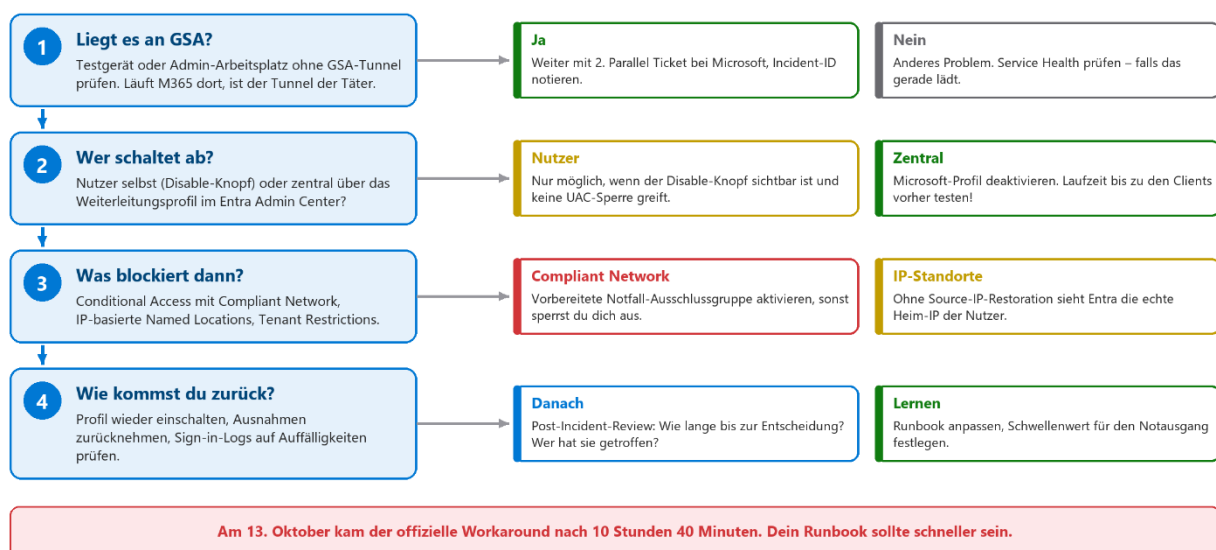


Abbildung 3: Entscheidungsbaum für das Notfall-Runbook bei einer GSA-Störung

Der zentrale Schalter

Im Entra Admin Center kannst du unter Global Secure Access die Weiterleitungsprofile einzeln deaktivieren. Schaltest du das Microsoft-Traffic-Profil ab, geht M365-Traffic direkt raus, ohne dass ein einziger Nutzer einen Knopf drücken muss. Sind alle Profile deaktiviert, zeigt der Client „Disabled by your organization“. Teste vorher, wie lange es dauert, bis deine Clients die geänderte Richtlinie tatsächlich ziehen. Wenn das eine halbe Stunde braucht, steht das ins Runbook, damit niemand nach fünf Minuten panisch den nächsten Schalter umlegt.

Die Notfall-Ausschlussgruppe

Für Compliant-Network-Richtlinien legst du eine leere Sicherheitsgruppe an, die in der Richtlinie bereits als Ausnahme eingetragen ist. Im Ernstfall nimmst du die betroffenen Nutzer auf, statt unter Druck eine Richtlinie umzubauen. Das ist schneller, nachvollziehbar und lässt sich sauber zurücknehmen. Wichtig: Wer darf die Gruppe befüllen? Das muss vorher klar sein, inklusive Vertretung. Der zuständige Kollege ist beim nächsten Ausfall garantiert im Urlaub. Auf Mallorca. Ohne Netz.

WICHTIG: Erst die Richtlinie, dann der Tunnel

Microsoft warnt selbst: Wer die GSA-Signalisierung für Conditional Access abschaltet, während Compliant-Network-Richtlinien aktiv sind, kann Nutzer unbeabsichtigt aussperren. Die Reihenfolge im Notfall lautet daher: Ausschlussgruppe befüllen, kurz prüfen, dann das Weiterleitungsprofil deaktivieren. Andersherum produzierst du in Rekordzeit den zweiten Ausfall des Tages.

Monitoring, das nicht von Microsoft abhängt

Am 13. Oktober war die Service-Health-Ansicht für manche Admins selbst gestört. Richte deshalb externe Signale ein: synthetische Tests, die regelmäßig Outlook im Web und SharePoint über GSA und parallel ohne GSA abrufen. Läuft der direkte Weg und der Tunnel nicht, hast du deine Diagnose in Minuten statt in Stunden. Ergänzend helfen Dienste, die Microsoft-Statusmeldungen mitschneiden und alarmieren, sowie ein Blick in die GSA-Traffic-Logs. Und ein ganz analoges Signal: ein Helpdesk, der bei drei gleichlautenden Anrufen in zehn Minuten eskaliert, statt das dritte Ticket „Outlook langsam“ zu schließen.

TIPP: Spiel es einmal durch – an einem Dienstag

Nimm eine Pilotgruppe von zehn Leuten, kündige den Test an und simuliere den Ausfall: Profil deaktivieren, Ausschlussgruppe befüllen, Zeit stoppen, Rückweg testen. Wenn das beim ersten Mal 90 Minuten dauert, ist das kein Misserfolg, sondern der Grund, warum du es geübt hast.

Maßnahme	Warum	Bis wann
Bestandsaufnahme: Wer läuft über welches Weiterleitungsprofil?	Ohne Überblick keine gezielte Abschaltung	sofort
Client-Registry-Werte dokumentieren (HideDisableButton, RestrictNonPrivilegedUsers)	Bestimmt, ob Nutzer sich selbst helfen können	sofort
Notfall-Ausschlussgruppe in Compliant-Network-Richtlinien eintragen	Verhindert Selbstaussperrung beim Abschalten	Ende Oktober
Break-Glass-Konten prüfen und Anmeldung testen	Admins müssen im Ernstfall ins Entra Admin Center	Ende Oktober
Synthetisches Monitoring mit und ohne GSA	Diagnose ohne Statusseite	November
Runbook mit Entscheidungsbefugnis und Schwellenwert	Wer schaltet wann ab, wer schaltet zurück?	November
Notfallübung mit Pilotgruppe	Laufzeiten kennen, bevor es ernst wird	Dezember

Und noch ein Wort zur Entscheidungsbefugnis, weil das in der Praxis am häufigsten klemmt. Ein Ausfall wie dieser ist keine rein technische Frage, sondern eine Abwägung zwischen Sicherheit und Arbeitsfähigkeit. Die darf nicht der Admin im zweiten Lehrjahr allein treffen, der Angst hat, dass ihm das Abschalten später als Sicherheitsvorfall angekreidet wird. Leg fest: Ab 30 Minuten bestätigter Störung entscheidet die IT-Leitung oder ihr Vertreter, mit Freigabe durch den Informationssicherheitsbeauftragten. Schriftlich, vorher. Dann wird aus elf Stunden Lähmung eine Stunde Störung mit sauberem Protokoll.

Häufig gestellte Fragen

Was war die Ursache der Global-Secure-Access-Störung am 13. Oktober 2026?

Microsoft nannte in den Zwischenmeldungen einen Teil der Global-Secure-Access-Infrastruktur, der unterhalb der akzeptablen Leistungsschwellen arbeitete. Behoben wurde die Störung durch Umleiten des Traffics auf gesunde Infrastruktur und gezielte Neustarts, ein ausführlicher Post-Incident-Report lag zunächst nicht vor.

Wie kann ich Global Secure Access im Notfall für alle Nutzer deaktivieren?

Im Microsoft Entra Admin Center lassen sich unter Global Secure Access die Weiterleitungsprofile zentral deaktivieren, etwa nur das Microsoft-Traffic-Profil. Der Traffic für Microsoft 365 geht dann direkt ins Internet, wobei es eine Weile dauern kann, bis alle Clients die Änderung übernehmen.

Warum werde ich nach dem Deaktivieren von Global Secure Access von Microsoft 365 blockiert?

Wahrscheinlich verlangt eine Conditional-Access-Richtlinie ein „Compliant Network“, also eine Anmeldung über den Global-Secure-Access-Tunnel des eigenen Tenants. Ohne Tunnel scheitern neue Anmeldungen, deshalb braucht es für den Notfall eine vorbereitete Ausschlussgruppe in dieser Richtlinie.

Können Nutzer den Global-Secure-Access-Client selbst ausschalten?

Standardmäßig ja, über die Schaltfläche „Disable“ im Infobereich, und der Client bleibt dann bis zum Wiedereinschalten oder Neustart deaktiviert. Administratoren können die Schaltfläche per Registry-Wert HideDisableButton ausblenden oder mit RestrictNonPrivilegedUsers lokale Administratorrechte für das Abschalten verlangen.

Welche Microsoft-365-Dienste waren von der GSA-Störung betroffen?

Microsoft nannte unter anderem Outlook, Outlook im Web, OneDrive, SharePoint Online, Microsoft Teams und Windows 365 Cloud PCs. Betroffen waren ausschließlich Nutzer, die Microsoft 365 über Global Secure Access erreichen, zuletzt nur noch in Deutschland.