Die 20 größten Exchange-Skandale, Ausfälle und Sicherheitslücken in 10 Jahren

> Microsoft Exchange gehört seit Jahrzehnten zu den wichtigsten E-Mail-Plattformen für Unternehmen. Gleichzeitig war die Plattform immer wieder von **kritischen Sicherheitslücken, erfolgreichen Angriffen und teilweise weltweiten Ausfällen** betroffen.
>
> Diese Übersicht zeigt die 20 bedeutendsten Vorfälle rund um **Exchange Server On-Premises, Exchange-Hybridumgebungen und Exchange Online in Microsoft 365**. Berücksichtigt werden bekannte Schwachstellen, tatsächliche Angriffe, Cloud-Ausfälle und organisatorische Versäumnisse. Stand der Übersicht: **17. September 2026**.

Bewertung:

? Kritische Sicherheitslücke oder erfolgreicher Angriff
? Hohes Sicherheits- oder Verfügbarkeitsrisiko
? Bedeutender Ausfall, Softwarefehler oder Governance-Vorfall

Inhaltsverzeichnis

Exchange Server On-Premises und Hybrid

☐ 1. ProxyLogon und HAFNIUM: massenhafte Übernahme von Exchange-Servern

Zeitpunkt: März 2021
Einstufung: ? Kritische Zero-Day-Angriffskette
Betroffen: Exchange Server 2010, 2013, 2016 und 2019

Die Schwachstellen CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 und CVE-2021-27065 ermöglichten den Zugriff auf Exchange-Server ohne reguläre Anmeldung. Angreifer konnten Schadcode mit SYSTEM-Rechten ausführen, E-Mails entwenden und dauerhafte Webshells auf den Servern hinterlegen.

Besonders kritisch war, dass die spätere Installation der Updates bereits vorhandene Webshells nicht automatisch beseitigte. Ein gepatchter Server konnte daher weiterhin kompromittiert sein.

> **Prüfpunkte:**
>
> - Aktuelles Cumulative Update und sämtliche Security Updates installieren.
> - IIS-, ECP-, OAB- und EWS-Protokolle forensisch untersuchen.
> - Exchange-Verzeichnisse auf unbekannte ASPX-Webshells prüfen.
> - Administrator- und Dienstkonten nach einer Kompromittierung ändern.

Quellen: **Microsoft Incident Guidance** | **CISA Advisory AA21-062A**

☐ 2. ProxyShell: vollständige Remoteübernahme

Zeitpunkt: 2021
Einstufung: ? Aktiv ausgenutzte RCE-Angriffskette
CVE: CVE-2021-34473, CVE-2021-34523 und CVE-2021-31207

ProxyShell kombinierte drei Schwachstellen. Angreifer konnten die Exchange-Authentifizierung umgehen, Berechtigungen erweitern und schließlich Schadcode oder Webshells ausführen. Die Angriffskette wurde später unter anderem zur Verteilung von Ransomware und Kryptominern eingesetzt.

- OWA und ECP nicht unnötig direkt im Internet veröffentlichen.
- IIS-Protokolle auf ungewöhnliche Autodiscover- und ECP-Aufrufe prüfen.
- Exchange PowerShell auf erforderliche Systeme und Administratoren begrenzen.

Quellen: **CVE-2021-34473** | **CVE-2021-34523** | **CVE-2021-31207**

☐ 3. ProxyNotShell: erneut ausgenutzte Exchange-Zero-Days

Zeitpunkt: September 2022
Einstufung: ? SSRF und Remote Code Execution
CVE: CVE-2022-41040 und CVE-2022-41082

Ein Angreifer mit gültigen Zugangsdaten konnte über Autodiscover und die Exchange-PowerShell Befehle auf dem Server ausführen. Microsoft stellte zunächst mehrfach angepasste URL-Rewrite-Regeln bereit, bevor vollständige Sicherheitsupdates verfügbar waren.

- Aktuelle Exchange-Sicherheitsupdates installieren.
- Frühere provisorische Rewrite-Regeln kontrollieren und dokumentieren.
- Exchange PowerShell nicht allgemein aus dem Internet erreichbar machen.

Quelle: **Microsoft-Analyse zu ProxyNotShell**

☐ 4. CVE-2025-53786: Vom lokalen Exchange in die Microsoft-Cloud

Zeitpunkt: August 2025
Einstufung: ? Kritische Hybrid-Rechteausweitung

In bestimmten Hybridbereitstellungen konnte ein Angreifer mit administrativem Zugriff auf den lokalen Exchange-Server möglicherweise seine Berechtigungen auf Exchange Online ausweiten. Damit konnte die Kompromittierung eines On-Premises-Servers zum Sicherheitsvorfall in der Cloud werden.

- Aktuelle Exchange-Sicherheitsupdates installieren.
- Microsofts dedizierte Exchange-Hybridanwendung einrichten.
- Alte gemeinsam verwendete Service Principals entfernen.
- Entra- und Exchange-Auditlogs auf ungewöhnliche App-Zugriffe prüfen.

Quellen: **Microsoft CVE-2025-53786** | **CISA-Warnung**

☐ 5. OWASSRF: Umgehung bisheriger ProxyNotShell-Schutzmaßnahmen

Zeitpunkt: Dezember 2022
Einstufung: ? Remote Code Execution
CVE: CVE-2022-41080 und CVE-2022-41082

Die Angriffskette zeigte, dass die bisherigen URL-Filter und ProxyNotShell-Schutzmaßnahmen nicht alle Angriffswege beseitigten. Angreifer konnten über Outlook Web Access erneut die Exchange-PowerShell erreichen und Code ausführen.

Quellen: **CVE-2022-41080** | **CVE-2022-41082**

☐ 6. CVE-2020-0688: statische kryptografische Schlüssel

Zeitpunkt: Februar 2020
Einstufung: ? Remote Code Execution nach Anmeldung

Exchange verwendete bekannte statische Schlüssel zur Absicherung von ViewState-Daten. Ein Angreifer mit den Zugangsdaten eines beliebigen Postfachbenutzers konnte präparierte Daten erzeugen und unter Umständen Code mit SYSTEM-Rechten ausführen.

Quellen: **Microsoft CVE-2020-0688** | **Microsoft Security Update**

☐ 7. PrivExchange: von Exchange zum Domain Admin

Zeitpunkt: 2018 und 2019
Einstufung: ? NTLM Relay und Rechteausweitung
CVE: CVE-2018-8581

Durch weitreichende Exchange-Berechtigungen im Active Directory und einen NTLM-Relay-Angriff konnte die Kompromittierung des Exchange-Servers bis zur vollständigen Übernahme der Windows-Domäne führen.

- LDAP Signing und Channel Binding aktivieren.
- NTLM-Verwendung soweit möglich reduzieren.
- Exchange-Berechtigungen im Active Directory überprüfen.

Quelle: **Microsoft CVE-2018-8581**

☐ 8. CVE-2024-21410: NTLM-Leak und Rechteausweitung

Zeitpunkt: Februar 2024
Einstufung: ? Kritische Rechteausweitung
CVSS: 9,8

Präparierte Nachrichten konnten die Weitergabe von NTLM-Informationen auslösen. Diese ließen sich möglicherweise für Relay-Angriffe verwenden. Microsoft aktivierte im Rahmen der Absicherung Extended Protection standardmäßig für aktuelle Exchange-Versionen.

- Extended Protection überprüfen.
- Ausgehende SMB-Verbindungen ins Internet blockieren.
- NTLM-Relay-Schutz für LDAP, IIS und weitere Dienste aktivieren.

Quelle: **Microsoft CVE-2024-21410**

☐ 9. Exchange-Y2K22: Mailtransport zum Jahreswechsel gestoppt

Zeitpunkt: 1. Januar 2022
Einstufung: ? Schwerer Softwarefehler

Die Versionsnummer der Exchange-Malware-Scanning-Engine passte ab dem Jahr 2022 nicht mehr in den vorgesehenen Integer-Wert. Dadurch liefen Transportwarteschlangen voll und E-Mails wurden nicht mehr

zugestellt.

- Transportwarteschlangen kontinuierlich überwachen.
- Nicht nur Port 25, sondern die tatsächliche Zustellung testen.
- Notfallverfahren für Probleme mit der Malware-Engine dokumentieren.

Quelle: **Analyse des Exchange-Y2K22-Fehlers**

☐ 10. CVE-2026-42897: aktiv ausgenutzte OWA-Sicherheitslücke

Zeitpunkt: Mai bis Juli 2026
Einstufung: ? Aktiv ausgenutzte Schwachstelle
CVSS: 8,1

Eine präparierte E-Mail konnte beim Öffnen in Outlook Web Access unter bestimmten Bedingungen JavaScript im Browserkontext des Benutzers ausführen. Betroffen waren Exchange 2016, Exchange 2019 und Exchange Server Subscription Edition.

- Juli-2026-Sicherheitsupdates installieren.
- Exchange Emergency Mitigation Service aktivieren.
- OWA nicht mit Internet Explorer oder IE-Modus verwenden.

Quellen: **Microsoft CVE-2026-42897** | **Exchange-Sicherheitsupdates 2026** | **CISA KEV-Hinweis**

Exchange Online und Microsoft 365

☐ 11. Storm-0558: gestohlener Microsoft-Schlüssel öffnet Behördenpostfächer

Zeitpunkt: Mai bis Juni 2023
Einstufung: ? Cloud-Sicherheits- und Governance-Skandal

Ein chinesischer Angreifer verwendete einen erlangten Microsoft-Consumer-Signaturschlüssel und eine fehlerhafte Tokenprüfung. Damit wurden Tokens erzeugt, die den Zugriff auf Exchange Online und Outlook Web Access ermöglichten. Betroffen waren etwa 25 Organisationen, darunter westliche Regierungsstellen.

- Unified Audit Log und MailItemsAccessed aktivieren.
- Ausreichende Aufbewahrungsdauer für Auditdaten konfigurieren.
- Ungewöhnliche OWA-, Graph- und EWS-Zugriffe überwachen.

Quelle: **Microsofts Storm-0558-Bericht**

☐ 12. Midnight Blizzard kompromittiert Microsofts eigene E-Mail-Umgebung

Zeitpunkt: November 2023 bis Januar 2024
Einstufung: ? Sicherheits- und Governance-Skandal

Russische Angreifer kompromittierten per Password Spray ein altes Microsoft-Testkonto ohne MFA. Anschließend missbrauchten sie privilegierte OAuth-Anwendungen und erhielten Zugriff auf Exchange-Online-Postfächer von Führungskräften sowie Mitarbeitern aus Sicherheits- und Rechtsabteilungen.

- MFA ausnahmslos auch für Test- und Dienstkonten erzwingen.
- Ungenutzte Mandanten und Service Principals entfernen.
- ApplicationImpersonation und full_access_as_app kontrollieren.
- OAuth-Anwendungen mit Zugriff auf EWS oder Microsoft Graph überwachen.

Quellen: **Microsoft Incident Guidance** | **Bericht zum Angriff**

☐ 13. Weltweite Outlook- und Exchange-Störung EX1464935

Zeitpunkt: September 2026
Einstufung: ? Weltweiter Cloud-Ausfall

Anwender konnten sich nicht anmelden, Postfächer synchronisierten nicht und Nachrichten ließen sich teilweise weder versenden noch empfangen. Die Störung betraf eine zentrale Komponente der Exchange-Online-Infrastruktur.

- Incident EX1464935 für SLA- und Risikonachweise archivieren.
- Notfallkommunikation unabhängig von Microsoft 365 bereithalten.
- Anwender vor dem mehrfachen Versand wartender E-Mails warnen.

Quelle: **Bericht zur weltweiten Outlook-Störung**

☐ 14. Exchange Online und Outlook fallen weltweit aus

Zeitpunkt: 25. und 26. November 2024
Einstufung: ? Großer Cloud-Ausfall

Eine Änderung in Microsofts Infrastruktur beeinträchtigte Exchange Online, Outlook und die Kalenderfunktionen von Teams. Die Wiederherstellung dauerte deutlich länger als ursprünglich erwartet.

- Kritische Kontaktdaten außerhalb von Exchange speichern.
- Alternative Kommunikationswege regelmäßig testen.
- Service-Health-Meldungen für mögliche SLA-Ansprüche archivieren.

Quelle: **AP-Bericht zum Microsoft-365-Ausfall**

☐ 15. Fehlerhafte Codeänderung legt Microsoft 365 lahm

Zeitpunkt: 1. März 2025
Einstufung: ? Globaler Cloud-Ausfall
Incident: MO1020913

Outlook, Exchange und weitere Microsoft-365-Dienste waren über mehrere Stunden nicht erreichbar. Microsoft führte den Vorfall auf eine problematische Codeänderung zurück und stellte die Dienste durch einen Rollback wieder her.

Quelle: **Analyse zu MO1020913**

☐ 16. 14-stündiger Exchange-Online-Ausfall

Zeitpunkt: 11. und 12. September 2025
Einstufung: ? Regionaler Großausfall
Incident: EX1151485

Anmeldung, Mailboxzugriff, Kalender und Mailzustellung waren vor allem in Nordamerika beeinträchtigt. Als Ursache wurde eine unerwartet hohe CPU-Auslastung in Teilen der Exchange-Online-Infrastruktur genannt.

Quelle: **Bericht zu EX1151485**

☐ 17. Exchange Online durch Layer-7-DDoS beeinträchtigt

Zeitpunkt: Juni 2023
Einstufung: ? Angriff auf die Verfügbarkeit

Die Gruppe Storm-1359 führte HTTP-Flood-, Cache-Bypass- und Slowloris-Angriffe gegen Microsoft-Dienste durch. Microsoft bestätigte zeitweise Einschränkungen der Verfügbarkeit, sah jedoch keine Hinweise auf den Zugriff auf Kundendaten.

Quelle: **Microsofts DDoS-Stellungnahme**

☐ 18. Infrastrukturfehler bei Exchange Online im Januar 2026

Zeitpunkt: 22. Januar 2026
Einstufung: ? Großer regionaler Ausfall

Teile der nordamerikanischen Infrastruktur verarbeiteten den Datenverkehr nicht mehr korrekt. Benutzer erhielten unter anderem den temporären SMTP-Fehler `451 4.3.2`. Microsoft musste den Verkehr auf funktionsfähige Infrastruktur umleiten.

- Eigene Systeme müssen temporäre SMTP-Fehler automatisch wiederholen.
- Monitoring muss 4xx-Verzögerungen von endgültigen 5xx-Fehlern unterscheiden.
- Bei Cloud-Ausfällen nicht vorschnell lokale Outlook-Profile löschen.

Quelle: **Bericht zum Ausfall**

☐ 19. Exchange Online verschiebt legitime E-Mails in Quarantäne

Zeitpunkt: Februar 2026
Einstufung: ? Fehlkonfiguration der Filter

Eine aktualisierte URL-Erkennungsregel stufte legitime Links und Nachrichten fälschlicherweise als Phishing ein. Dadurch wurden geschäftliche E-Mails weltweit in die Quarantäne verschoben.

- Quarantänevolumen und plötzliche Ausschläge überwachen.
- Freigaben von Nachrichten revisionssicher dokumentieren.
- Automatische Klassifizierungen regelmäßig durch Stichproben prüfen.

Quelle: **Bericht zur Fehlklassifizierung**

☐ 20. Unzureichende Transparenz bei Exchange-Online-Ausfällen

Zeitraum: fortlaufend
Einstufung: ? Governance- und Cloudrisiko

Detaillierte Ursachen, Incident-IDs und Abschlussberichte sind häufig nur im tenantbezogenen Microsoft-365-Admin-Center sichtbar. Öffentliche Statusseiten bieten oftmals keine dauerhaft verfügbare und vollständige Historie. Das erschwert unabhängige Ursachenanalysen, SLA-Nachweise und langfristige Risikobewertungen.

- Service-Health-Meldungen automatisiert archivieren.
- Incident-ID, Beginn, Ende und geschäftliche Auswirkung dokumentieren.
- Eigene externe Verfügbarkeitsmessungen einsetzen.
- Mögliche SLA-Gutschriften fristgerecht beantragen.

Weiterführende Informationen: **Microsoft 365 Service Health** | **Microsoft Graph Service Communications API**

Was zeigen die Exchange-Sicherheitsvorfälle?

Die Vorfälle belegen nicht, dass grundsätzlich nur eine Betriebsform sicher oder unsicher ist. Vielmehr verschieben sich die Verantwortlichkeiten und Risiken:

- **Exchange On-Premises:** Das größte Risiko ist ein ungepatchter und direkt aus dem Internet erreichbarer Server.
- **Exchange Hybrid:** Eine lokale Kompromittierung kann über Vertrauensstellungen auch die Cloud gefährden.
- **Exchange Online:** Microsoft übernimmt Plattformbetrieb und Updates, nicht jedoch alle Risiken durch Identitäten, OAuth-Apps, Fehlkonfigurationen und kompromittierte Benutzerkonten.
- **Cloudabhängigkeit:** Bei einer zentralen Störung können Kunden die Fehlerbehebung kaum beeinflussen und sind auf Microsofts Kommunikation angewiesen.

Kompakte Exchange-Sicherheitscheckliste

? Unterstützte Exchange-Version und aktuelles CU verwenden

? Security Updates zeitnah installieren

? Exchange Health Checker regelmäßig ausführen

? OWA und ECP nicht unnötig direkt veröffentlichen

? MFA für Administratoren und Benutzer erzwingen

? Alte Konten, Test-Tenants und OAuth-Anwendungen entfernen

? ApplicationImpersonation und App-only-Berechtigungen kontrollieren

? Extended Protection aktivieren und überprüfen

? IIS-, Exchange-, Entra- und Unified-Audit-Logs zentral sichern

? Mailfluss und Transportwarteschlangen aktiv überwachen

? Notfallkommunikation außerhalb von Microsoft 365 vorhalten

? Service-Health-Vorfälle und SLA-relevante Ausfälle archivieren

Häufige Fragen zu Exchange-Sicherheit und Ausfällen

Ist Exchange Online sicherer als ein eigener Exchange-Server?

Exchange Online reduziert das Risiko ungepatchter Server und nimmt dem Unternehmen einen großen Teil des Plattformbetriebs ab. Dafür entstehen neue Abhängigkeiten von Microsoft, der Cloudidentität und der Verfügbarkeit der Microsoft-365-Infrastruktur. Automatisch sicher ist Exchange Online daher nicht.

Ist ein aktueller Exchange-Server noch direkt angreifbar?

Jede öffentlich erreichbare Anwendung kann neue Schwachstellen enthalten. Exchange sollte deshalb vollständig aktualisiert, überwacht und möglichst durch zusätzliche Zugriffsschutzmaßnahmen abgesichert werden.

Reicht es, Exchange-Sicherheitsupdates zu installieren?

Nein. Wurde eine Schwachstelle bereits ausgenutzt, beseitigt das Update möglicherweise die Sicherheitslücke, aber nicht automatisch Webshells, gestohlene Zugangsdaten oder andere Hintertüren. In diesem Fall ist eine forensische Untersuchung erforderlich.

Kann ein lokaler Exchange die Microsoft-Cloud gefährden?

Ja. Besonders in Hybridumgebungen existieren Vertrauensstellungen zwischen lokalem Exchange, Entra ID und Exchange Online. CVE-2025-53786 zeigte, dass eine lokale Kompromittierung unter bestimmten Voraussetzungen bis in die Cloud reichen kann.

Was passiert bei einem Exchange-Online-Ausfall?

Kunden können die eigentliche Störung nicht selbst reparieren. Wichtig sind deshalb alternative Kommunikationswege, ein lokaler Outlook-Cache, dokumentierte Notfallverfahren und die Archivierung der Microsoft- Service-Health-Meldungen.

Hinweis: Die Rangfolge ist eine redaktionelle Bewertung anhand von technischer Schwere, tatsächlicher Ausnutzung, Reichweite und betrieblicher Auswirkung. Die Übersicht ersetzt keine individuelle Sicherheitsanalyse einer Exchange- oder Microsoft-365-Umgebung.

Letzte Aktualisierung: 17. September 2026

Version #1
Erstellt: 2026-09-17 10:12:04 UTC von Christian Zengel (sysops GmbH)
Zuletzt aktualisiert: 2026-09-17 10:13:27 UTC von Christian Zengel (sysops GmbH)