Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

Microsoft Exchange: Gefährdung für zehntausende Server nach Support-Ende für Versionen 2016 und 2019

BITS-B Nr. 2025-287772-1032, Version 1.0, 28.10.2025

Kritikalität*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:CLEAR: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Bitte prüfen Sie selbstständig, für welche Stellen in Ihrer Organisation die hier genannten Informationen relevant sind und leiten Sie das Schreiben entsprechend weiter – sofern die TLP-Einstufung dies zulässt.

Sachverhalt

Die Unterstützung des Herstellers Microsoft für die Produkte Exchange-Server 2016 und 2019 endete planmäßig am 14.10.2025 [MS24]. Seitdem werden keine Sicherheitsupdates mehr für diese Versionen bereitgestellt.

Dennoch laufen in Deutschland aktuell noch 92% der dem BSI bekannten rund 33.000 on-premise Exchange-Server mit offen aus dem Internet erreichbarem Outlook Web Access mit Version 2019 und älter.

* 1 / Grau: Maßnahmen sollten in absehbarer Zeit erwogen werden. Keine wesentlichen Beeinträchtigungen zu erwarten.
2 / Gelb: Maßnahmen müssen zeitnah ergriffen werden. Temporäre Beeinträchtigungen des Regelbetriebs möglich.
3 / Orange: Maßnahmen müssen unverzüglich ergriffen werden. Massive Beeinträchtigung des Regelbetriebs möglich.
4 / Rot Maßnahmen müssen sofort ergriffen werden. Geschäftskritische Beeinträchtigung möglich.

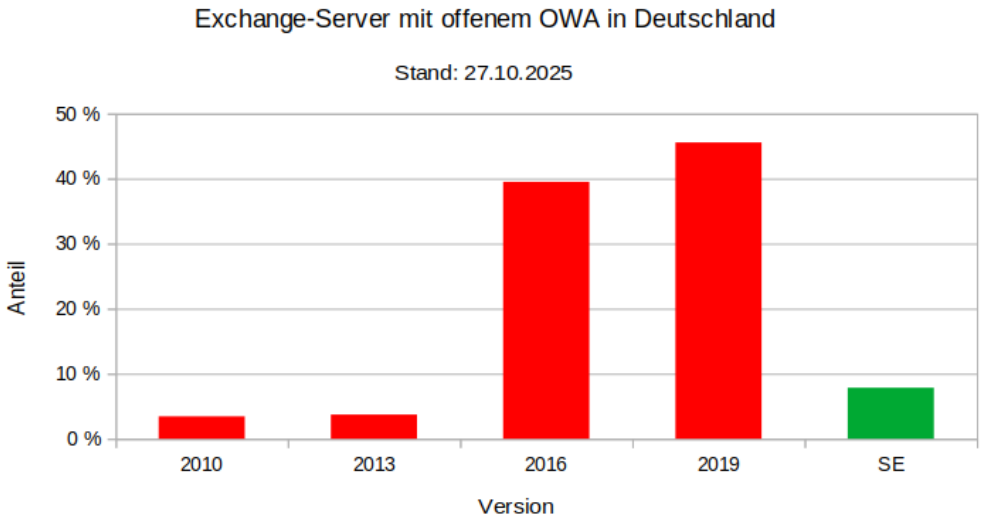

Abb. 1: Prozentualer Anteil der verschiedenen Exchange-Server-Versionen in Deutschland

Neben tausenden Unternehmen ist unter anderem auch eine Vielzahl von Krankenhäusern und Arztpraxen, Schulen und Hochschulen, Sozialdiensten, Anwalts- und Steuerkanzleien, Stadtwerken und Kommunalverwaltungen betroffen.

Das CERT-Bund des BSI informiert Netzbetreiber in Deutschland bereits seit langer Zeit regelmäßig zu IP-Adressen in ihren Netzen, unter denen sich Exchange-Server befinden, die noch mit den nicht mehr unterstützen Versionen 2010 und 2013 laufen. Ab sofort werden auch die Versionen 2016 und 2019 entsprechend gemeldet.

Bewertung

Sollte demnächst eine kritische Schwachstelle in Microsoft Exchange bekannt werden – wie es in den letzten Jahren mehrfach der Fall war – kann diese nicht mit einem Sicherheitsupdate geschlossen werden. Die betroffenen Exchange-Server müssen dann ggf. umgehend vom Netz genommen werden, um eine Kompromittierung zu vermeiden. Die Folge wäre eine massive Einschränkung der Kommunikationsfähigkeit der betroffenen Organisationen.

Die Kompromittierung eines Exchange-Server führt aufgrund flacher Netzwerkstrukturen und unzureichender Segmentierung und Härtung häufig schnell zu einer vollständigen Kompromittierung des kompletten Netzwerks der Betroffenen, was einen Abfluss sensibler Informationen, die Verschlüsselung von Daten mittels Ransomware und anschließender Lösegeldforderung sowie wochenlange Produktionsausfälle bedeuten kann.

Da auf Exchange-Servern personenbezogenen Daten verarbeitet werden, stellt der weitere Betrieb veralteter Versionen zudem einen Verstoß gegen die DSGVO dar.

Maßnahmen

Microsoft stellt mit dem Extended Security Update Programm (ESU) gegen zusätzliche Bezahlung noch bis zum 14.04.2026 weitere potenzielle Sicherheitsupdates für kritische Schwachstellen zur Verfügung [MS25]. Dies erfordert jedoch zusätzliche finanzielle Mittel und verschiebt erforderliche Maßnahmen zum Upgrade bzw. zur Migration der Systeme nur um maximal sechs Monate.

Das BSI rät Betreibern betroffener Exchange-Server daher, umgehend ein Upgrade auf Version SE oder eine Migration auf eine alternative Lösung durchzuführen.

Das BSI empfiehlt, webbasierte Dienste des Exchange-Servers wie Outlook Web Access grundsätzlich nicht offen aus dem Internet erreichbar zu machen, sondern den Zugriff auf vertrauenswürdige Quell-IP-Adressen zu beschränken oder über ein VPN abzusichern. Das BSI stellt ein IT-Grundschutz-Hilfsmittel mit weiteren Informationen zur Absicherung von E-Mail-Systemen bereit [BSI21].

Referenzen

[BSI21] E-Mail-System: Sicherer Remote-Zugang
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Hilfsmittel_Remote_Zugang_E_Mail_System_v1.pdf

[MS24] Supportende für Office und Exchange Server 2016 und 2019 – was du jetzt tun musst
https://www.microsoft.com/de-de/techwiese/news/supportende-fuer-office-und-exchange-server-2016-und-2019--was-du-jetzt-tun-musst.aspx

[MS25] Announcing Exchange 2016 / 2019 Extended Security Update program
https://techcommunity.microsoft.com/blog/exchange/announcing-exchange-2016--2019-extended-security-update-program/4433495

Versionsverlauf

Version 1.0 — 28.10.2025

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs), welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1. Was ist das Traffic Light Protokoll?
   Das vom BSI verwendete TLP basiert auf der Definition der TLP Version 2.0 des „Forum of Incident Response and Security Team“ (FIRST). Es dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen durch Regelungen der Weitergabe. Eine unbefugte Weitergabe kann eine Verletzung der Vertraulichkeit, eine Rufschädigung, eine Beeinträchtigung der Geschäftstätigkeit oder datenschutzrechtliche Belange zur Folge haben. Im Zweifelsfall ist immer in Absprache mit dem Informationsersteller zu handeln.
2. Welche Einstufungen existieren?
   - **TLP:CLEAR: Unbegrenzte Weitergabe**
     Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.
   - **TLP:GREEN: Organisationsübergreifende Weitergabe**
     Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe (bspw. Angehörige der Cybersecurity-Community) angehören.
   - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Weitergabe**
     Der Empfänger darf die Informationen, welche als TLP:AMBER gekennzeichnet sind, an seine Partner weitergeben, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen. Eine Weitergabe von den Partnern an Dritte ist nicht erlaubt und auch innerhalb der Partnerorganisationen gilt das Prinzip „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
     - **TLP:AMBER+STRICT: Eingeschränkte interne Weitergabe**
       Die Einstufung von Informationen als TLP:AMBER+STRICT beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers. Jegliche Weitergabe darüber hinaus ist untersagt. Es gilt „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
   - **TLP:RED: Persönlich, nur für benannte Empfänger**
     Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden.
3. Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?
   Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.
4. Was passiert, wenn ich die Einstufung nicht beachte?
   Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:CLEAR eingestufte Informationen aus dem Kreis der Verpflichteten.

Hinweis zu Upload-, Prüf- und Übersetzungsdiensten

TLP-eingestufte Dokumente (außer TLP:CLEAR) dürfen nicht auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort ggf. Dritten zugänglich gemacht werden.