Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

SCHWACHSTELLE | **GEFÄHRDUNG** | VORFALL | IT-ASSETS

Tausende Microsoft-Exchange-Server in Deutschland weiterhin für kritische Schwachstellen verwundbar

CSW-Nr. 2024-223466-1032, Version 1.0, 26.03.2024

IT-Bedrohungslage*: 3 / Orange

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.

Sachverhalt

Microsoft Exchange ist ein weit verbreiteter E-Mail- und Groupware-Server. Microsoft stellt regelmäßig Sicherheitsupdates für Exchange zur Verfügung, mit denen unter anderem kritische Sicherheitslücken geschlossen werden. Das BSI hat in der Vergangenheit mehrfach zu Schwachstellen in Exchange gewarnt und empfohlen, die zur Verfügung gestellten Sicherheitsupdates zeitnah einzuspielen.

Aktuell werden in Deutschland rund 45.000 Microsoft-Exchange-Server mit offen aus dem Internet erreichbarem Outlook Web Access (OWA) betrieben. Nach Erkenntnissen des BSI laufen davon ca. 12% noch mit Exchange 2010 oder 2013. Für diese Versionen werden bereits seit Oktober 2020 bzw. April 2023 keine Sicherheitsupdates mehr zur Verfügung gestellt.

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb: IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange: Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

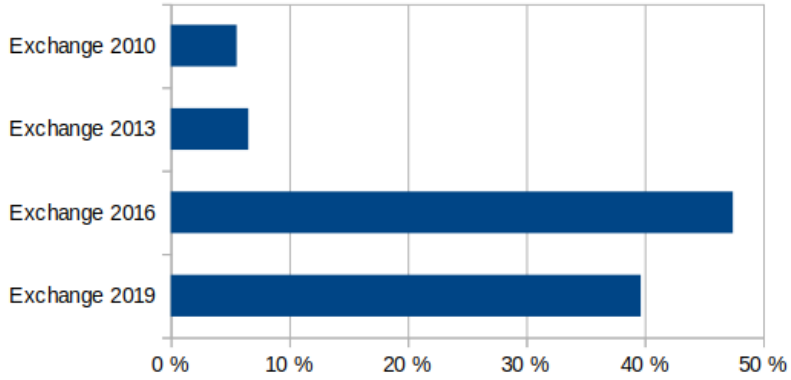

Abb. 1: Anteile der Exchange-Versionen in Deutschland

Von den Servern mit den aktuellen Versionen Exchange 2016 oder 2019 sind heute ca. 28% auf einem mindestens vier Monate alten Patch-Stand und dadurch für eine oder mehrere kritische Schwachstellen verwundbar, welche einem entfernten Angreifenden die Ausführung beliebigen Programmcodes auf dem Opfersystem ermöglichen (Remote Code Execution, RCE). Dies entspricht rund 25% aller Exchange-Server in Deutschland.

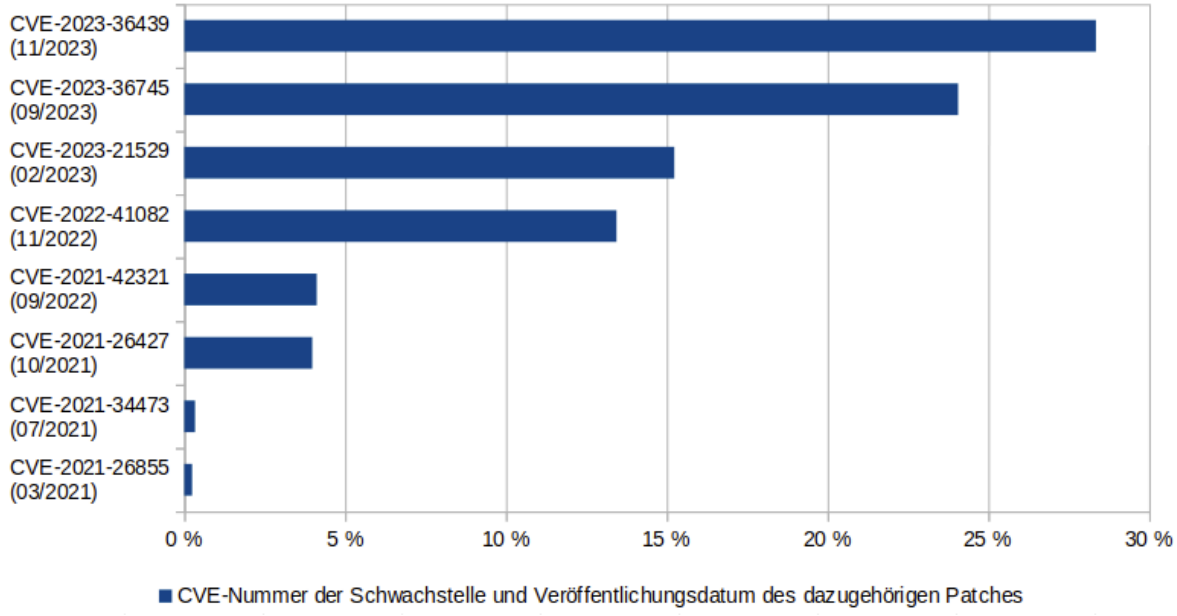

Abb. 2: Kritische Schwachstellen der Exchange-Server 2016/2019 in Deutschland

Am 13.02.2024 wurde eine weitere kritische Schwachstelle in Exchange bekannt (CVE-2024-21410). Diese wird jedoch nicht durch einen Patch geschlossen. Stattdessen kann die Ausnutzung der Schwachstelle unter anderem durch Aktivierung der "Extended Protection for Authentication" (EPA) verhindert werden. Die Anfälligkeit eines Servers für diese Schwachstelle hängt jedoch von verschiedenen Faktoren ab, die von außen nicht eindeutig bewertet werden können. Das Cumulative Update 14 für Exchange 2019 aktiviert die Extended Protection standardmäßig. Dieses Update ist auf ca. 15% der Exchange-Server in Deutschland installiert.

Mit den am 12.03.2024 veröffentlichten Sicherheitsupdates wurde eine weitere RCE-Schwachstelle (CVE-2024-26198) behoben. Eine abschließende Bewertung des von dieser Schwachstelle ausgehenden Risikos steht noch aus, daher wird diese hier noch nicht berücksichtigt.

Bewertung

Rund 12% der Microsoft-Exchange-Server in Deutschland laufen mit den schon seit geraumer Zeit nicht mehr unterstützten Versionen 2010 oder 2013 und weisen daher mehrere kritische Sicherheitslücken auf. Der weitere Betrieb dieser Exchange-Server am Internet ist daher als hochriskant anzusehen.

Weitere 25% der Exchange-Server laufen zwar mit den aktuellen Versionen 2016 oder 2019, sind aber auf einem veralteten Patch-Stand, sodass sie ebenfalls eine oder mehrere kritische Sicherheitslücken aufweisen.

Für 48% der Exchange-Server kann keine eindeutige Aussage hinsichtlich der Verwundbarkeit für die kritische Schwachstelle CVE-2024-21410 getroffen werden. Diese Systeme sind noch verwundbar, sofern die Betreiber nicht die seit August 2022 zur Verfügung stehende Extended Protection aktiviert oder andere Schutzmaßnahmen getroffen haben.

15% der Server laufen mit der neuesten Version Exchange 2019 CU14, mit der die Extended Protection standardmäßig aktiviert ist. Diese Server sind daher mit hoher Wahrscheinlichkeit nicht für die Schwachstelle CVE-2024-21410 verwundbar.

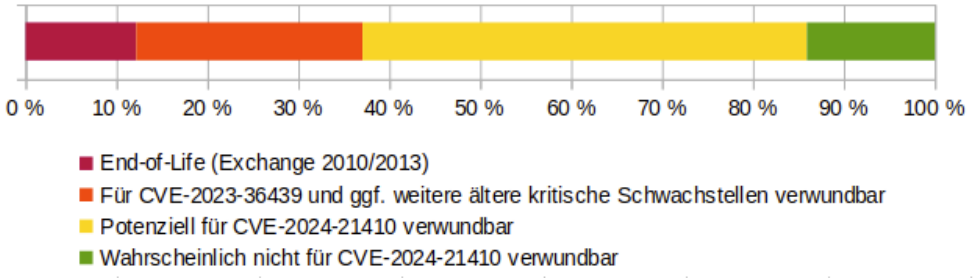

Abb. 3: Status der Exchange-Server in Deutschland bzgl. ihrer Verwundbarkeit

Insgesamt sind aktuell **mindestens 37% der Exchange-Server in Deutschland** (und in vielen Fällen damit auch die dahinterliegenden Netzwerke) **stark gefährdet**. Dies entspricht ca. 17.000 Systemen.

Das BSI geht jedoch davon aus, dass die Extended Protection bisher nur auf einem Teil der potenziell verwundbaren Systeme von den Betreibern aktiviert wurde und somit **tatsächlich noch über die Hälfte aller Exchange-Server in Deutschland für kritische Schwachstellen verwundbar ist**.

Betroffen sind inbesondere viele Schulen und Hochschulen, Kliniken, Arztpraxen, Pflegedienste und andere medizinische Einrichtungen, Rechtsanwälte und Steuerberater, Kommunalverwaltungen sowie mittelständische Unternehmen.

Die kritischen Schwachstellen können von Angreifenden ausgenutzt werden, um beliebigen Programmcode auf betroffenen Exchange-Servern auszuführen. Zahlreiche Cyberkriminelle sowie staatliche Akteure nutzen mehrere der Schwachstellen aktiv aus, um darüber zum Beispiel Spam zur Verbreitung von Schadsoftware zu versenden, in interne Netzwerke der Opfer einzudringen und sensible Informationen auszuspähen oder gar das Active Directory vollständig zu kompromittieren und Ransomware zur Verschlüsselung von Daten mit anschließender Erpressung und Lösegeldforderung auszurollen.

Bereits 2021 warnte das BSI mehrfach vor der aktiven Ausnutzung kritischer Schwachstellen in Microsoft Exchange und rief zeitweise die IT-Bedrohungslage "rot" aus [BSI2021a]. Trotzdem hat sich die Lage seitdem nicht verbessert, da viele Betreiber von Exchange-Servern weiterhin sehr nachlässig handeln und zur Verfügung stehende Sicherheitsupdates nicht zeitnah einspielen.

Maßnahmen

Betreiber von Microsoft-Exchange-Servern sollten regelmäßig überprüfen, ob Ihre Systeme auf dem aktuellen Patch-Stand sind und die monatlichen Sicherheitsupdates zeitnah einspielen. Die derzeit aktuellen Versionen sind:

- Exchange Server 2019 CU14 Mar24SU (Build-Nummer 15.2.1544.9)
- Exchange Server 2019 CU13 Mar24SU (Build-Nummer 15.2.1258.32)
- Exchange Server 2016 CU23 Mar24SU (Build-Nummer 15.1.2507.37)

Weiterhin sollte zum Schutz vor Ausnutzung der aktuellen kritischen Sicherheitslücke CVE-2024-21410 sichergestellt werden, dass die "Extended Protection for Authentication" aktiviert ist oder andere Schutzmaßnahmen getroffen wurden. Weitere Informationen hierzu finden Sie in der entsprechenden Schwachstellen-Warnung [BSI2024].

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 [BSI2021b].

CERT-Bund informiert Netzbetreiber in Deutschland bereits seit längerer Zeit tagesaktuell automatisiert per E-Mail zu IP-Adressen in ihren Netzen, unter denen sich bekannte verwundbare Exchange-Server befinden. Provider werden gebeten, ihre jeweils betroffenen Kunden entsprechend zu informieren. Ob, wann und in welcher Form die Provider ihre Kunden benachrichtigen, ist jedoch erfahrungsgemäß sehr unterschiedlich.

Über die verwundbaren Exchange-Server hinaus meldet CERT-Bund täglich automatisiert mehrere zehntausend weitere verwundbare Systeme sowie Schadprogramm-Infektionen und andere Sicherheitsvorfälle an Netzbetreiber in Deutschland. Die automatisierten Benachrichtigungen werden üblicherweise an den für die jeweils betroffene IP-Adresse beim RIPE NCC (der europäischen Vergabestelle für IP-Adressen) eingetragenen Abuse-Kontakt gesendet. Organisationen, die eigene öffentliche IP-Netze betreiben, sollten überprüfen, ob für ihre Netze ein entsprechender Abuse-Kontakt beim RIPE NCC eingetragen ist [RIPE2024].

Links

[BSI2021a] Kritische Schwachstellen in Exchange-Servern
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Server/Microsoft-Exchange_Schwachstelle/schwachstelle_exchange_server_node.html

[BSI2021b] 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

[BSI2024] Microsoft Exchange: Aktive Ausnutzung einer Zero-Day-Schwachstelle
https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2024/2024-214205-1032.pdf

[RIPE2024] RIPEstat Abuse Contact Finder
https://stat.ripe.net/specials/abuse

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.