Der Bayerische Landesbeauftragte für den Datenschutz
gemeinsam mit dem Bayerischen Landesamt für Datenschutzaufsicht

MICROSOFT EXCHANGE SECURITY CHECK & INCIDENT RESPONSE

Version 1.0, Stand:12.03.2021

Gemeinsame Herausgeber:

Bayerisches Landesamt für Datenschutzaufsicht
Promenade 18
91522 Ansbach

Tel.: 0981 180093-0
E-Mail: poststelle@lda.bayern.de
Web: www.lda.bayern.de

Der Bayerische Landesbeauftragte für den Datenschutz
Wagmüllerstraße 18
80538 München

Tel.: 089 212672-0
E-Mail: poststelle@datenschutz-bayern.de
Web: www.datenschutz-bayern.de

Ausgangslage

Durch Informationen von Microsoft und des Bundesamts für Sicherheit in der Informationstechnik (BSI) wurde Anfang März 2021 bekannt, dass vier Zero-Day-Sicherheitslücken in Microsoft Exchange Servern existieren. Diese Lücken machen Unternehmen und andere Verantwortliche über das Internet angreifbar, sobald sie Microsoft Exchange Server unter einer bestimmten Konfiguration einsetzen. Das BSI stuft die Gesamtsituation als kritisch ein, da bereits eine flächendeckende Ausnutzung stattfand und somit die Wahrscheinlichkeit einer Kompromittierung der verwundbaren Systeme als realistisch anzusehen ist. Dem Bayerischen Landesamt für Datenschutzaufsicht (BayLDA) und dem Bayerischen Landesbeauftragten für den Datenschutz (BayLfD) liegen bereits mehrere hundert Meldungen nach Art. 33 DS-GVO vor, bei denen eine Kompromittierung nachgewiesen werden konnte. Es handelt sich somit um keine abstrakte, sondern um eine akute Gefährdung, bei der zeitnahes Handeln erforderlich ist. Microsoft stellt sowohl Patches zum Schließen der Sicherheitslücken zur Verfügung gestellt als auch Anleitungen und Möglichkeiten, den eigenen Server gezielt auf eine Infektion hin zu prüfen. Das BSI bietet zudem Unterstützung zur Detektion und Reaktion.

Ziel dieses Dokuments

Bei verantwortlichen Betreibern der jeweiligen Exchange Server besteht zuweilen Ungewissheit, ob es auf Grund der eigenen Verwundbarkeit auch zu einer erfolgreichen Cyberattacke mit den damit verbundenen negativen Auswirkungen auf die eigene IT-Sicherheit, den Datenschutz und den weiteren Betrieb der Organisation gekommen ist. Dieses Dokument soll Verantwortliche bei der Aufarbeitung in einfachen Schritten begleiten, ohne dabei eine starre chronologische Abfolge aufzudrängen. Es handelt sich weder um einen verbindlichen noch um einen abschließenden Maßnahmenkatalog. Stattdessen ist das Dokument insbesondere als Ergänzung zu den ohnehin schon zahlreichen Selbsthilfe-Angeboten im Internet zu verstehen – allerdings mit der Besonderheit, den datenschutzrechtlichen Blickwinkel der Art. 32 bis 34 DS-GVO zu integrieren.

Betroffene Systeme

Nach aktuellem Kenntnisstand sind folgende Systeme betroffen:

- Exchange Server 2010 (RU 31 für Service Pack 3)
- Exchange Server 2013 (CU 23)
- Exchange Server 2016 (CU 19, CU 18)
- Exchange Server 2019 (CU 8, CU 7)

Folgende Schwachstellen führen in Kombination zur Verwundbarkeit:

- CVE-2021-26855: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855
- CVE-2021-26857: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26857
- CVE-2021-26858: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26858
- CVE-2021-27065: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-27065

A. Sofortmaßnahmen zur Verhinderung von weiteren Angriffen

Hinweis: Voraussetzung zur angemessenen Reaktion und Durchführung einzelner Sicherheitsmaßnahmen ist technisch versiertes Personal.

1. Im Rahmen der akuten Gefährdungslage erfolgen die meisten Angriffe über HTTPS-Zugriffe auf TCP-Port 443 zu Exchange Servern. Aus diesem Grund sollten zunächst diese Außenverbindungen geschlossen werden, um diesen Angriffsvektor aktiv zu unterbinden:
   - Sofortige Sperrung des Webzugriffs/Ports 443 auf dem Exchange Server, um externen Zugriff über die verwundbaren Webdienste auf den Mailserver zu unterbinden (über OWA, Autodiscover, Active Sync).
   - Weiteres Vorgehen nach der Sperrung des Ports 443 planen: Präventiv sollte künftig der Zugang nur über eine VPN-Verbindung etabliert werden können, um den Server vor unbefugten externen Zugriffen zu schützen. Der Port 443 bleibt insbesondere über das Internet für Externe gesperrt. Der Mailtransport über TCP-Port 25 (SMTP) von und nach extern ist von dieser Einschränkung nicht betroffen. Eine Beschränkung der externen Erreichbarkeit des Mailservers über die Firewall (mittels Port 25) kann entsprechend erfolgen.
2. Prüfung der aktuell installierten Exchange-Server-Version (Abgleich des Patch Levels) zur Feststellung des Handlungsbedarfs. Anschließendes Einspielen der verfügbaren Security Patches von Microsoft je nach System:
   - Server 2010 Service Pack 3
   - Server 2013 Kumulatives Update (CU 23)
   - Server 2016 Kumulatives Update (CU 18, CU 19)
   - Server 2019 Kumulatives Update (CU 7, CU 8)

   Die notwendigen Updates haben keinen Einfluss auf die Funktionsfähigkeit. Die Dokumentation von Microsoft zum Einspielen der Updates ist zu beachten:
   https://techcommunity.microsoft.com/t5/exchange-team-blog/released-march-2021-exchange-server-security-updates/ba-p/2175901

B. Überprüfung auf technische Kompromittierung

Hinweis: Sollten bereits Anhaltspunkte für eine Kompromittierung des Exchange Servers vorliegen, sind Maßnahmen einzuleiten, um eine versehentliche Datenveränderung zu vermeiden und Nachweise bspw. in Form einer Vollsicherung oder Snapshots des Exchange-Systems zu sichern. Hier ist bereits eine Rücksprache mit der Polizei bzw. der Zentralen Ansprechstelle Cybercrime (ZAC) empfehlenswert, um spätere Ermittlungen nicht zu erschweren: https://polizei.bayern.de/lka/kriminalitaet/internet/index.html/294473

Das BSI Dokument „Microsoft Exchange Schwachstellen – Detektion und Reaktion" liefert eine fortlaufend aktualisierte Darstellung geeigneter Schritte zur Überprüfung der Exchange Server auf Kompromittierung:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Vorfaelle/Exchange-Schwachstellen-2021/MSExchange_Schwachstelle_Detektion_Reaktion.pdf

1. Automatische, toolunterstützte Prüfung der Exchange Server, z. B. auf Webshells, als Hinweis auf einen bereits stattgefundenen, unbefugten Zugriff. Diese Prüfung erfolgt mit Hilfe von geeigneten Scan-Tools von Microsoft und dem Einsatz von Security Scannern (d. h. sowohl spezifische Erkennungswerkzeuge als auch klassische Virenscanner):

- Einsatz des Detektionsskripts von Microsoft (Test-ProxyLogon.ps1) zur Analyse, um die Server nach Indizien für die Ausnutzung des Exploits zu untersuchen:
  https://github.com/microsoft/CSS-Exchange/tree/main/Security
  Nach Berücksichtigung der in der Anleitung von Microsoft beschriebenen Vorgehensweise ist das Ergebnis zu analysieren. Hier können sich bereits klare Anzeichen einer Kompromittierung ergeben. Eine entsprechende Dokumentation der Ergebnisse ist auch hier für die datenschutzrechtliche Bewertung erforderlich.
- Durchführung einer vollständigen Systemprüfung (Dateisystem, Registry, Prozesse, Arbeitsspeicher etc.) durch eine Antiviren-Lösung mit aktuellen Signaturen (z. B. hinsichtlich „Winnet") oder dem integrierten Microsoft Defender. Ein Einsatz des Microsoft Safety Scanners (MSERT) auf dem Exchange Server ist ebenso möglich:
  https://docs.microsoft.com/de-de/windows/security/threat-protection/intelligence/safety-scanner-download
  Möglicherweise wurden durch die Antiviren-Lösung bereits Bedrohungen festgestellt, sodass erste Anhaltspunkte für einen Angriff vorliegen. Denkbar ist jedoch auch, dass keine Webshells gefunden werden, weil die verwendete Antiviren-Lösung eventuelle Funde bereits gelöscht hat. Daher sind Logs der Antiviren-Lösung ebenfalls zu überprüfen.

2. Manuelle Überprüfung der Exchange Server:
   - Analyse der Log-Files und des Dateisystems:
     Befinden sich verdächtige Dateien in den Verzeichnissen?
     Wurden in den relevanten Zeiträumen Auffälligkeiten in den Logs registriert?
     - Priorität 1: Aktueller Zeitraum vom 2. März 2021 bis heute
     - Priorität 2: Jüngere Vergangenheit vom November 2020 bis 1. März 2021
   - Kontrolle der bekannten Verzeichnisse, in denen Webshells abgelegt sein könnten. Die Dateinamen der bisher in diesem Zusammenhang aufgedeckten Webshells lauten:
     - Web.aspx
     - Help.aspx
     - Document.aspx
     - errorEE.aspx
     - errorEEE.aspx
     - errorEW.aspx
     - errorFF.aspx
     - healthcheck.aspx
     - aspnet_www.aspx
     - aspnet_client.aspx
     - xx.aspx
     - shell.aspx
     - aspnet_iisstart.aspx
     - one.aspx
   - Zudem werden Pfade nach Webshells untersucht. Webshells wurden bisher unter folgenden Pfaden beobachtet:
     - C:\inetpub\wwwroot\aspnet_client\
     - C:\inetpub\wwwroot\aspnet_client\system_web\
     - %PROGRAMFILES%\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\
     - C:\Exchange\FrontEnd\HttpProxy\owa\auth
3. Analyse des ein- und ausgehenden Datenverkehrs der Exchange Server durchführen (z. B. Firewall-Log).

4. Erste Untersuchung des verbundenen Active Directory im Hinblick auf veränderte, privilegierte Berechtigungen oder Accounts.
5. Änderung von Benutzerpasswörtern und administrativen Passwörtern im Active Directory. Exchange Server besitzen meist hohe Rechte im Active Directory. Weitgehende Angriffe könnten zur Kompromittierung der gesamten Domäne führen.

C. Maßnahmen bei Kompromittierungsverdacht

1. Spätestens jetzt den Incident Response Modus bzw. bekannte Ablaufpläne bei IT-Sicherheitsvorkommnissen und Datenschutzverletzungen starten.
2. Eine Meldung nach Art. 33 DS-GVO bei der zuständigen Datenschutzaufsichtsbehörde ist durchzuführen, sobald ein Risiko für betroffene Personen hinreichend wahrscheinlich ist. Davon ist bei einer festgestellten Kompromittierung auf Grund der bekannten Gefährdungslage auszugehen.
3. Snapshots und Logs für forensische Analyse sichern. Wichtig bleibt, Rücksprache mit der Polizei zu führen, um eine versehentliche Datenveränderung zu vermeiden. Anschließend Erstellung von Nachweisen in Form von Log-Files, Screenshots und Binaries etc.
4. Sicherung des Serverstands zu forensischen Zwecken (Full Backup, VM).
5. Falls möglich: Quarantäne des betroffenen Mailservers zum Einleiten der Forensik.
6. Falls möglich: Memory Dump erstellen.
7. Backup-Restore auf einen nicht-kompromittierten Stand durchführen und eine damit verbundene Neuinstallation (Hinweis: Es gibt diverse Möglichkeiten, nach einem Angriff den Exchange wieder in Betrieb zu nehmen, die jedoch vom konkreten Schadensbild und der weiteren unternehmerischen Ausrichtung abhängen.).
8. Je nachdem, wie die Schwachstellen ausgenutzt und das IT-System kompromittiert wurde, ist ggf. eine vollständige Säuberung des IT-Systems von Schadcode-Fragmenten möglich (Entfernung aller Webshells (ASPX), Backdoors (Webshell, Powercat) und Scheduled Tasks). Weitere Scans sind durchzuführen.
9. Ggf. Neuerstellung des virtuellen Verzeichnisses für das Offline-Adressbuch (OAB).
10. Detailuntersuchung des verbundenen Active Directory auf Anomalitäten, z. B. hinsichtlich neuer Accounts oder Account-Änderungen an administrativen Rollen. Durch die nachträgliche Kontrolle der privilegierten Berechtigungen im Active Directory und auf dem Exchange Server ist eine Kompromittierung des Active Directory mit den Rechten des Exchange Servers bzw. durch Hinzufügen von neuen Benutzern mit hochprivilegierten Rechten auszuschließen.
11. Abschalten alter Exchange Server bei Umzug auf Neuinstallationen.
12. Bei Vorliegen einer Cyberattacke ist eine Anzeige bei der zuständigen Polizei zu erstatten. Ansprechpartner für Nachfragen zu den Möglichkeiten der Strafverfolgung finden sich bei der Zentralen Ansprechstelle Cybercrime (ZAC) des Bayerischen Landeskriminalamtes (LKA):
    https://polizei.bayern.de/lka/kriminalitaet/internet/index.html/294473
    Hilfe für einen schnellen behördlichen Kontakt finden Sie bei der Cyberabwehr Bayern:
    https://www.lda.bayern.de/de/thema_cyberabwehr_bayern.html
13. Bei Anhaltspunkten für Betroffenheit von elektronischer Spionage, z. B. bei festgestelltem Datenabfluss, ist Kontakt zum Cyber-Allianz-Zentrum Bayern (CAZ) im Landesamt für Verfassungsschutz aufnehmen:
    E-Mail: caz@lfv.bayern.de, Tel.: 089/31201-222

D. Organisatorische Maßnahmen und Prävention

1. Den vorübergehenden Einsatz von beispielsweise Geo-Blocking für IP-Adressen und IP-Blacklisting in Erwägung ziehen. Hier entsprechende aktuelle Hinweise zu relevanten IP-Adressen von BSI und Microsoft verfolgen.
2. Einbindung eines externen Sicherheitsunternehmens, falls die eigenen Kapazitäten oder Fachkenntnisse zur weiteren Begleitung des Vorfalls nicht ausreichen.
3. Falls der Vorfall bei einem Dienstleister (Auftragsverarbeiter) stattgefunden hat: Weiterhin enger Austausch zur Aufarbeitung, da der Verantwortliche die Risikobewertung nach DS-GVO nur auf Grund der entsprechenden Untersuchungsergebnisse durchführen und dokumentieren kann.
4. Sensibilisierung der eigenen Nutzer/Mitarbeiter hinsichtlich entstehender Folgerisiken:
   - Sachgemäßer Umgang mit E-Mails
   - Erkennung von gefälschten E-Mails
   - Umgang mit Auffälligkeiten im Sinne einer Cyber Security Awareness
5. Organisatorische Vorbereitung zur schnellen Reaktion bei künftigen Sicherheitshinweisen (Fast Incident Response), insbesondere bei neuen Erkenntnissen zu nachgelagerten Verwundbarkeiten und Angriffsformen.
6. Internes Review des bestehenden Patch Management Prozesses. Eine einfache Checkliste zu wichtigen Punkten des Patch Managements findet sich hier: https://www.lda.bayern.de/media/checkliste/baylda_checkliste_patch_mgmt.pdf
7. Überprüfung der allgemeinen Schutzmaßnahmen zur Abwehr von Cyberbedrohungen im eigenen Betrieb. Eine Orientierung bietet bspw. die „Checkliste Cybersicherheit für medizinische Einrichtungen", da bis auf Kapitel 9 des Dokuments allgemeine Maßnahmen gelistet sind: https://www.lda.bayern.de/media/checkliste/baylda_checkliste_medizin.pdf
8. Überprüfung der Vollständigkeit und Wirksamkeit der eigenen Backup-Strategie. Sofern möglich und noch nicht praktiziert, zusätzliches Backup auf einem Offline-Datenträger erstellen (z. B. externe Festplatte).
9. Das Logging näher beobachten und steuern:
   - Überprüfung des Log-Levels auf Firewalls, Webproxies, Domain-Controller und Intrusion Detection Systemen.
   - Ggf. zeitweise Erhöhung des Umfangs bzw. des Log-Levels vor allem für Exchange Server und insbesondere Internetzugriffe, um eine regelmäßige Feinanalyse auf Grund der akuten Gefährdungslage durchführen zu können.
   - In Betracht ziehen: Zusätzliche Software für erweitertes Logging aufsetzen (Erhöhung des Log-Levels zur gesteigerten Prävention).
10. Verfolgung der aktuellen Entwicklung zur Bedrohungslage (insbesondere Veröffentlichungen von BSI und Microsoft).

E. Datenschutzrechtliches Ergebnis

Eine Sicherheitslücke alleine löst bekanntlich noch keine datenschutzrechtliche Meldeverpflichtung aus. Findet jedoch im konkreten Sachverhalt mit hinreichender Wahrscheinlichkeit eine Kompromittierung statt, ist davon auszugehen, dass die Vertraulichkeit und Integrität von Daten des Microsoft Exchange Servers nicht mehr gewährleistet werden kann. Auch die Integrität und Vertraulichkeit des Active Directory kann dadurch gefährdet sein. In allen Fällen, in denen eine Verwundbarkeit des Exchange Servers vorlag, ist somit immer entscheidend, welche Erkenntnisse durch die eingeleitete Untersuchung und Aufarbeitung tatsächlich gewonnen werden konnten. Liegt eine Kompromittierung vor bzw. haben sich die Hinweise darauf zumindest verdichtet? Dies ist Basis für die Fragestellung, ob eine meldepflichtige Datenschutzverletzung nach Art. 33 DS-GVO vorliegt oder nicht. Die maßgeblichen Feststellungen sind nach Art. 5 Abs. 2 DS-GVO (Rechenschaftspflicht) umfassend zu dokumentieren.

Folgende **Fallkonstellationen** (A bis F) sind im Hinblick auf personenbezogene Daten wesentlich:

- **Keine Meldepflicht nach Art. 33 DS-GVO**
  - A) Eine Verwundbarkeit des Exchange Servers war zwar gegeben, jedoch kann eine Kompromittierung nach umfangreichen Analysen ausgeschlossen werden. In diesem Fall liegt keine meldepflichtige Datenschutzverletzung vor, da die Schwachstelle mit hinreichender Wahrscheinlichkeit nicht ausgenutzt wurde (vgl. Art. 4 Nr. 12 DS-GVO).
  - B) Trotz festgestellter Kompromittierung kann ausgeschlossen werden, dass personenbezogene Daten betroffen sind. Es liegt demnach keine meldepflichtige Datenschutzverletzung vor, da keine personenbezogenen Daten betroffen sind (vgl. Art. 4 Nr. 12 DS-GVO).
  - C) Trotz festgestellter Kompromittierung und der Betroffenheit personenbezogener Daten kann ein Risiko für die betroffenen Personen nach DS-GVO ausgeschlossen werden. Es liegt somit keine meldepflichtige Datenschutzverletzung vor, da der Vorfall voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt (vgl. Art. 33 DS-GVO).

- **Meldepflicht nach Art. 33 DS-GVO**
  - D) Für den Fall, dass eine Verwundbarkeit gegeben war, aber man bislang nicht ausreichend nachprüfen konnte, in welchem Umfang eine Kompromittierung stattfand, ist von einer meldepflichtigen Datenschutzverletzung auszugehen, da den Sicherheitsbehörden Erkenntnisse vorliegen, dass verwundbare Server massenhaft und teils automatisiert angegriffen wurden.
  - E) Für den Fall, dass Updates sehr spät eingespielt wurden: Hier ist von einer meldepflichtigen Datenschutzverletzung auszugehen, da das Zeitfenster für einen erfolgreichen Angriff ausreichend groß war. Es wäre untypisch, wenn verwundbare, an das Internet angeschlossene Server längere Zeit trotz derart öffentlichem Bekanntwerden des Angriffsweges ohne Kompromittierung blieben. Hinsichtlich eines möglichen hohen Risikos können zu einem solchen Zeitpunkt keine nachhaltigen Aussagen getroffen werden. Daher muss der Sachverhalt weiter aufgearbeitet und die Meldung nach Art. 33 DS-GVO durchgeführt werden.
  - F) Falls eine Kompromittierung des verwundbaren Exchange Servers erkannt wurde: In den aller meisten Fällen hatten unbefugte Dritte (Angreifer) potentiell Zugriff auf Systeme und Dienste, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen. Eine Meldeverpflichtung bei der zuständigen Datenschutzaufsichtsbehörde besteht. Des Weiteren ist zu prüfen, ob betroffene Personen nach Art. 34 DS-GVO über die Verletzung ihrer personenbezogenen Daten zu unterrichten sind. Dies hängt u. a. entscheidend (aber nicht nur) von der Sensitivität der betroffenen personenbezogenen Daten ab. Folglich erfordert dieser Schritt eine äußerst sorgfältige, datenschutzrechtliche Bewertung und Vorgehensweise.

Weiterführende Links

- BayLDA Meldung einer Datenschutzverletzung nach Art. 33 DS-GVO für bayerische Verantwortliche aus dem nicht-öffentlichen Bereich: https://www.lda.bayern.de/datenschutzverletzung
- BayLfD Meldung einer Datenschutzverletzung nach Art. 33 DS-GVO für bayerische Verantwortliche aus dem öffentlichen Bereich: https://www.datenschutz-bayern.de/service/data_breach.html
- Cyberabwehr Bayern - Ansprechpartner zur Cybersicherheit in Bayern: https://www.lda.bayern.de/media/Behoerdenuebersicht_Cybersicherheitsvorfall.pdf
- BayLDA Cybersicherheit Checkliste mit Prüfkriterien nach Art. 32 DS-GVO: https://www.lda.bayern.de/media/checkliste/baylda_checkliste_medizin.pdf (ohne Kapitel 9)
- BayLDA Patch Management Checkliste nach Art. 32 DS-GVO: https://www.lda.bayern.de/media/checkliste/baylda_checkliste_patch_mgmt.pdf
- BayLDA FAQ zu Exchange Sicherheitslücken: https://www.lda.bayern.de/exchange
- Microsoft Detektionsskript: https://github.com/microsoft/CSS-Exchange/tree/main/Security
- Microsoft Safety Scanners (MSERT): https://docs.microsoft.com/de-de/windows/security/threat-protection/intelligence/safety-scanner-download
- Microsoft Security Response Center: https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/
- BSI-Cyber-Sicherheitswarnung: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-197772-1132.pdf
- BSI Microsoft Exchange Schwachstellen Detektion und Reaktion: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Vorfaelle/Exchange-Schwachstellen-2021/MSExchange_Schwachstelle_Detektion_Reaktion.pdf
- Zentrale Ansprechstelle Cybercrime (ZAC) des Bayerischen Landeskriminalamtes (LKA): https://polizei.bayern.de/lka/kriminalitaet/internet/index.html/294473

Hinweis:
Die Auflistung der Maßnahmen in diesem Dokument wurde mit freundlicher Unterstützung von Teilnehmern der Cyberabwehr Bayern erstellt.