MUNKER
Datenschutz

Datenschutz-Information zur Microsoft Exchange Sicherheitslücke

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat Anfang März über bestehende **Sicherheitslücken in Microsoft Exchange Servern** informiert. Diese Sicherheitslücken werden bereits sehr umfangreich von Hackern ausgenutzt.

Es ist davon auszugehen, dass alle **Nutzer von selbst betriebenen Microsoft Exchange Servern** 2013, 2016 oder 2019 (d.h. Installation auf den eigenen Servern) bereits betroffen sind, wenn diese über den Port 443 über das Internet für nicht-vertrauenswürdige Verbindungen erreichbar waren. Das betrifft also **auch die Installationen, die zwar in Rechenzentren betrieben werden**, dort aber vom Provider auf „lokalen" Servern installiert sind – fragen Sie hier bitte zur Sicherheit bei Ihrem Rechenzentrum nach.

Welche Gefahr besteht?

Durch die Sicherheitslücke ist es möglich, Ihre **Systeme mit Schadsoftware zu infizieren**, die in Exchange vorgehaltenen **E-Mail-Postfächer und Adressbücher komplett auszulesen** oder **Zugriff auf das Unternehmensnetzwerk** zu erlangen. Die Hacker haben u.a. auch die Möglichkeit, Hintertüren zu installieren, so dass auch nach Abwendung der Sicherheitslücken noch Zugriff auf Ihre Systeme bestehen könnte.

Es besteht also **dringender Handlungsbedarf**, um (weiteren) Schaden abzuwenden.

Was ist zu tun?

Wir empfehlen Ihnen dringend, **mit Ihrer IT-Abteilung oder dem IT-Systempartner zu klären**, ob Sie in den Kreis der potentiell betroffenen Microsoft Exchange Nutzer fallen.

Ist dies der Fall, müssen Sie umgehend sicherstellen, dass **der mittlerweile von Microsoft zur Verfügung gestellte Patch** zur Behebung der Sicherheitslücke installiert wurde. Sollte das noch nicht geschehen sein, ist dies sofort zu veranlassen.

Der sofortigen Installation der Sicherheitsupdates von Microsoft kommt auch zur Abwendung datenschutzrechtlicher Konsequenzen besondere Bedeutung zu. Zumindest das Bayerische Landesamt für Datenschutzaufsicht ist bereits in der Lage, von außen zu überprüfen, ob der Patch zum Schließen der Sicherheitslücke installiert wurde. **Das BayLDA hat bereits eine erste Prüfung zur Einschätzung der Gefahrenlage durchgeführt und weitere Prüfungen – dann mit Konsequenzen – angekündigt.**

Da bis zum Bekanntwerden der Sicherheitslücke bereits ein Angriff auf Ihr System erfolgt sein könnte, müssen Sie außerdem gemeinsam mit Ihrem Administrator prüfen, ob **Hinweise auf eine Kompromittierung des Systems** erkennbar sind.

MUNKER
Datenschutz

Datenschutzrechtliche Auswirkung

Wenn Ihre Microsoft Exchange Installation von der Problematik betroffen ist, besteht die sehr konkrete Gefahr, dass **unbefugte Dritte Zugriff auf personenbezogene Daten** in Ihrem System hatten oder noch haben und dass unter Umständen auch **personenbezogene Daten von Ihrem System abgezogen wurden** (Datenübermittlung). Im schlimmsten Fall ist z. B. Ihr kompletter E-Mail-Verkehr in fremde Hände geraten. Es handelt sich hierbei um eine Datenschutzpanne, die ggf. der Meldepflicht unterliegt.

Nach Aussage des Bayerischen Landesamts für Datenschutz gibt es zusätzlich die **Pflicht zur Meldung einer Datenpanne**, wenn das von Microsoft zur Verfügung gestellte Sicherheitsupdate nicht umgehend auf Ihren Systemen installiert wurde. Sie sollten daher unbedingt sicherstellen, dass Sie als Verantwortlicher unverzüglich die Installation aller Sicherheitsupdates bei Ihrem Administrator hinterfragt und – falls noch nicht geschehen – sofort veranlasst haben.

Die Aufsichtsbehörden anderer Bundesländer haben noch keine Mitteilungen zu konkreten Vorgehensweisen veröffentlicht. Es ist jedoch davon auszugehen, dass hier ähnliche Entscheidungen getroffen werden.

So finden Sie Anzeichen für einen eventuellen Angriff:

- Veranlassen Sie die **Prüfung alle Log-Dateien** Ihrer Mail- und Domänenkontroller auf auffällige Einträge durch Ihren Administrator (Achtung, hier ist ggf. in Ihrer IT-Richtlinie das 4-Augen-Prinzip vorgeschrieben).
- Führen Sie **Offline-Prüfungen aller gefährdeten Systeme** durch (Virenscans, Tests auf Schadsoftware).
- **Prüfen Sie Firewall- und IDS-Systeme auf Alarme**.
- **Prüfen Sie den Datenverkehr über den betroffenen Port 443** auf auffällige Vorkommnisse in den vergangenen Monaten.
- **Überwachen Sie Prozesse- und Benutzeranmeldungen an zentraler Stelle**, um unübliche Aktivitäten auf Ihrem System zu erkennen.

Mehr Informationen sowie Hilfestellung zur Prüfung der Systeme auf eventuelle Hackeraktivitäten finden Sie auf dieser Übersichtsseite von Microsoft. Leiten Sie den Link falls notwendig an Ihren Administrator weiter.

https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

MUNKER Datenschutz

Ich bin betroffen – was ist zu tun?

- **Informieren Sie uns per E-Mail** an datenschutz@munker.info, wenn Ihr System potentiell betroffen ist und Sie das notwendige Sicherheitsupdate nicht kurzfristig nach Bekanntwerden installiert haben.
- **Informieren Sie uns per E-Mail** an datenschutz@munker.info, wenn Sie aufgrund der oben beschriebenen Prüfungen davon ausgehen müssen, dass es unbefugten Zugriff Dritter auf Ihre Systeme oder nicht autorisierte Datenübermittlungen zu anderen Servern gab,
- Denken Sie daran, dass die **Meldung einer Datenpanne innerhalb von 72 Stunden** ab Bekanntwerden des Vorfalls durchgeführt werden muss – Sie sollten kurzfristig handeln.
- Sollte es zu einer Datenpanne gekommen sein, stimmen wir die weitere Vorgehensweise (Meldung an die Aufsichtsbehörde) mit Ihnen ab.
- Ergreifen Sie gemeinsam mit Ihrem IT-Administrator **alle notwendigen Maßnahmen, um die Integrität Ihrer Systeme wiederherzustellen** und den sicheren Betrieb zu gewährleisten.

Bitte klären Sie die oben geschilderten Sachverhalte tatsächlich zuerst mit Ihrem Systemadministrator, hierzu können wir Ihnen keine Hilfestellung bieten.

Sollten die beiden in der obenstehenden Strichaufzählung genannten Fälle bei Ihnen eingetreten sein, unterstützen wir Sie selbstverständlich bei der Prüfung einer Meldepflicht und, falls notwendig, der Durchführung der Meldung der bestehenden Datenpanne. Bitte wenden Sie sich dazu an die angegebene E-Mail-Adresse. So können wir eine schnelle Reaktion auch dann sicherstellen, wenn Ihr persönlicher Ansprechpartner aktuell nicht erreichbar ist.

Weitere Links zum Thema:

https://www.lda.bayern.de/de/thema_exchange_sicherheitsluecke.html

https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/210305_Exchange-Schwachstelle.html