Der Bayerische Landesbeauftragte für den Datenschutz
Bayerisches Landesamt für Datenschutzaufsicht

Sicherheitslücken bei Microsoft Exchange-Servern: Weiterhin akute Datenschutzrisiken

Gemeinsame Hilfestellungen der beiden bayerischen Datenschutzaufsichtsbehörden veröffentlicht

München und Ansbach, 18. März 2021

Durch Ausnutzung kritischer Sicherheitslücken in der Software des Microsoft Exchange-Servers ist es jüngst zu einer massiven, globalen Cyber-Angriffswelle gekommen, die auch im Freistaat Bayern erhebliche Datenschutzrisiken ausgelöst hat (siehe hierzu die Pressemitteilung des Bayerischen Landesamts für Datenschutzaufsicht vom 9. März 2021). Cyberkriminelle Angreifer können auf diese Weise über das Internet gezielt auf verwundbare Mailserver von Unternehmen und Behörden zugreifen. Bei anfälligen Systemen besteht seitdem die erhöhte Gefahr, dass unbefugt auf gespeicherte Daten wie E-Mails, Adressbücher oder Kalender zugegriffen wird. Zudem können diese Lücken weiter genutzt werden, um nachgelagerte Angriffe vorzubereiten, tiefer in interne IT-Systeme einzudringen sowie Schadcode, z. B. Verschlüsselungstrojaner, dort zu platzieren.

Nicht alltäglich an diesem Vorfall ist die hohe Anzahl der weltweit und auch in Deutschland angegriffenen Systeme. Betroffen ist auch eine Vielzahl bayerischer Unternehmen und öffentlicher, insbesondere staatlicher und kommunaler Stellen. Alleine im Zeitraum vom 9. bis zum 17. März 2021 registrierten die beiden bayerischen Datenschutzaufsichtsbehörden in diesem Zusammenhang über 750 eingegangene Meldungen über Datenschutzverletzungen nach Art. 33 Datenschutz-Grundverordnung (DSGVO).

Prof. Dr. Thomas Petri, der Bayerische Landesbeauftragte für den Datenschutz, betont: „Bei einem erfolgreichen Angriff auf den Microsoft Exchange-Server kann der gesamte E-Mail-Verkehr für den Angreifer zugänglich sein. Gerade bei öffentlichen Stellen können hierdurch in großem Umfang selbst interne E-Mails mit möglicherweise besonders schützenswerten Daten, etwa mit medizinischen oder steuerlichen Inhalten, beispielsweise aber auch Daten des Jugendamts, Unbefugten zugänglich werden.“ Auch wenn viele bayerische öffentliche Stellen zwischenzeitlich die Lücken geschlossen haben und nicht jeder Exchange-Server zwingend angegriffen wurde, ist dennoch festzustellen, dass die Angriffswelle noch nicht abgeschlossen ist. „Das alleinige Einspielen der Patches reicht bei Weitem nicht aus. Es liegen bereits ausreichende Erkenntnisse vor, dass diverse Gruppen von Angreifern nach wie vor versuchen, weitere Schadsoftware wie Verschlüsselungstrojaner zu installieren und Daten zu Erpressungs- oder anderen Missbrauchszwecken abzugreifen. Eine erhöhte Wachsamkeit ist auch nach dem Durchführen der wichtigsten Sicherheitsmaßnahmen unerlässlich“, so Prof. Dr. Thomas Petri.

Michael Will, Präsident des Bayerischen Landesamts für Datenschutzaufsicht, ergänzt: „Die bisherigen Meldungen zeigen uns, dass in den allermeisten Fällen nicht nur der abstrakte Verdacht eines unbefugten Zugriffs auf den eigenen Exchange-Server besteht, sondern tatsächlich konkrete Anhaltspunkte für eine Kompromittierung vorliegen. Nicht immer muss dabei ein Datenabfluss erkannt und somit die Vertraulichkeit der relevanten Daten in Frage gestellt werden, in zahlrei-

chen Fällen ist schon die Integrität der Datenverarbeitung durch eine Manipulation nicht mehr gewährleistet.“ Immerhin sind aber bereits erste Erfolge der intensiven Warnungen und Aufklärungsmaßnahmen der Sicherheits- und Datenschutzbehörden erkennbar. Michael Will stellt fest: „Die Warnmeldungen der vergangenen Woche scheinen bei den meisten Betreibern angekommen zu sein. Wir nehmen auch in zahlreichen Beratungsgesprächen wahr, dass sich viele Verantwortliche ihrer gesetzlichen Verpflichtung bewusst sind, für eine sichere Datenverarbeitung zu sorgen. Trotzdem bleibt bei so manchen die Ungewissheit, welche Schadensausmaße eine solche Attacke am Ende haben wird.“

Aufgrund der nach wie vor akuten Bedrohungslage haben die beiden bayerischen Datenschutzaufsichtsbehörden eine gemeinsame „Praxishilfe zu Microsoft Exchange Sicherheitslücken“ veröffentlicht, die im Detail ausführt, welche Prüfungsschritte und Maßnahmen bei der Aufarbeitung unterstützen können. Zudem legt sie dar, ab wann die Meldepflicht nach Art. 33 DSGVO bei der zuständigen Datenschutzaufsichtsbehörde besteht. Insbesondere weisen die beiden bayerischen Datenschutzaufsichtsbehörden auf folgende Punkte hin:

- Bayerische Unternehmen und öffentliche Stellen, die die Sicherheits-Patches vom 3. März 2021 nicht zeitnah oder noch nicht eingespielt haben und deren Exchange-Server aus dem Internet ohne weitere Schutzmaßnahmen (wie etwa VPN) erreichbar sind, müssen davon ausgehen, dass ihre Systeme aufgrund der mittlerweile vergangenen Zeit mit hoher Wahrscheinlichkeit kompromittiert sind und somit massive Sicherheits- und Datenschutzrisiken bestehen. Sie müssen dringend die in der Praxishilfe dargestellten Abhilfemaßnahmen ergreifen. Zudem haben sie den Umfang der Ausnutzung der Schwachstelle sowie die Meldepflicht nach Art. 33 DSGVO zu prüfen.

  Werden die erforderlichen Maßnahmen weiterhin nicht ergriffen und sind Zugriffe auf besonders schutzwürdige personenbezogene Daten erfolgt, werden die bayerischen Datenschutzaufsichtsbehörden aufsichtsrechtliche Maßnahmen ergreifen.

- Betroffene bayerische öffentliche Stellen und private Unternehmen, die Risiken für die bei ihnen gespeicherten personenbezogenen Daten nicht belastbar ausschließen können, müssen unverzüglich ihrer Meldepflicht nach Art. 33 DSGVO nachkommen. Das Vorhandensein der vom BSI genannten Webshells oder weiterer Schadsoftware auf dem eigenen Server ist in diesem Fall ein deutliches Indiz für eine bestehende Meldepflicht, da nicht nur die Vertraulichkeit der personenbezogenen Daten, sondern auch die Integrität sowie gegebenenfalls die Verfügbarkeit des für die Datenverarbeitung wichtigen Systems gefährdet sein kann.

Zu den Sicherheitslücken bei Microsoft Exchange-Servern haben die beiden bayerischen Datenschutzaufsichtsbehörden zudem einen gemeinsamen Frage-und-Antwort-Bereich (FAQ) online zur Verfügung gestellt.

Prof. Dr. Thomas Petri
Der Bayerische Landesbeauftragte für den Datenschutz

Michael Will
Präsident des Bayerischen Landesamts für Datenschutzaufsicht

Aufsichtsbehörde	Hausanschrift	Postanschrift	Telefon / Fax	E-Mail / Internet
Der Bayerische Landesbeauftragte für den Datenschutz	Wagmüllerstraße 18 80538 München	Postfach 22 12 19 80502 München	089/212672-0 089/212672-50	poststelle@datenschutz-bayern.de; https://www.datenschutz-bayern.de
Bayerisches Landesamt für Datenschutzaufsicht	Promenade 18 91522 Ansbach	Postfach 1349 91504 Ansbach	0981/180093-0 0981/180093-800	poststelle@lda.bayern.de; https://www.lda.bayern.de