Sicherheitslücken bei Microsoft Exchange-Mail-Servern: Akuter Handlungsbedarf für bayerische Unternehmen

Mittwoch, 10 März 2021

https://www.datenschutz.de/sicherheitsluecken-bei-microsoft-exchange-mail-servern-akuter-handlungsbedarf-fuer-bayerische-unternehmen/

– BayLDA empfiehlt: Patchen, prüfen, melden! –

Pressemitteilung des Bayerischen Landesamts für Datenschutzaufsicht vom 09.03.2021

Nach der aktuellen Presseveröffentlichung des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist eines klar: Die neu bekannt gewordenen Schwachstellen in Microsoft Exchange-Mail-Servern betreffen auch eine Vielzahl deutscher Firmen. Eine Ad-hoc-Online-Untersuchung des BayLDA hat alleine im ersten Prüflauf eine dreistellige Zahl von Unternehmen identifiziert, deren Systeme auch mehrere Tage nach den ersten Sicherheitswarnungen weiterhin akut gefährdet sind. BayLDA-Präsident Will: „Wir sehen mit großer Sorge, dass trotz eindringlicher Warnungen durch die Sicherheitsbehörden und sofortiger Hilfestellungen durch Microsoft immer noch verwundbare Mail-Server im Netz zu finden sind. Für die von uns identifizierten Unternehmen besteht jetzt akuter Handlungsbedarf. Die betroffenen Systeme müssen umgehend gepatcht und dann umfassend überprüft werden. Für Unternehmen, die bis jetzt untätig geblieben sind, gehen wir von einer meldepflichtigen Datenschutzverletzung aus.“

Schwachstellen als IT-Bestandteil
Ein professioneller Umgang mit Sicherheitslücken sollte längst zum Alltag jedes IT-Betriebes gehören. Unabhängig von der Art und der Größe des Unternehmens ist es vor allem bei IT-Systemen, die über das Internet erreichbar sind, neben einer richtigen Konfiguration von entscheidender Bedeutung, bekannt gewordene Schwachstellen möglichst zeitnah zu beheben. Automatisierte Scans quer durch das Internet ermöglichen es ansonsten Angreifern aus der Ferne, auf Knopfdruck einen Überblick über verwundbare Server zu erhalten und nach Belieben Cyberattacken darauf zu starten. Das Zeitfenster zum Beheben von Sicherheitslücken ist somit meistens sehr gering.

BSI informiert über neue kritische Schwachstellen in Microsoft Exchange
Mit der Pressemitteilung vom 05.03.2021 informierte das BSI über eine neue, außerordentlich kritische Gefährdungslage, die bei den auch in Deutschland sehr weit verbreiteten Exchange Servern sofortiges Handeln der betroffenen Unternehmen erfordert. Durch die kombinierte Anwendung der neuen Exchange-Schwachstellen ist eine Code-Ausführung aus der Ferne für Angreifer möglich. Das BSI geht davon aus, dass die so verwundbaren Systeme mit hoher Wahrscheinlichkeit bereits attackiert und mit Schadsoftware infiziert sind.

Erfolgreiche Attacken setzen allerdings unter anderem voraus, dass eine nicht-vertrauenswürdige Verbindung zu einem Exchange Server etabliert werden kann, z. B. über Outlook Web Access. Laut Informationen des BSI sind Server, welche nur per VPN erreichbar sind oder eben solche nicht-vertrauenswürdige Verbindungen blockieren, nicht betroffen. Dennoch geht das BSI nach bisherigen

Veröffentlichungen von einer fünfstelligen Anzahl an betroffenen Systemen alleine in Deutschland aus.

Microsoft Patches einspielen
Das Einspielen der von Microsoft bereitgestellten Updates sollte von Exchange-Administratoren unverzüglich durchgeführt werden. Microsoft stellt mittlerweile zudem ein eigenes Prüf-Skript für betroffene Betriebe zur Verfügung (siehe unten in „Weiterführende Links“). Mit diesem können die Systemadministratoren der Firmen Anhaltspunkte dafür finden, ob der eigene Exchange Server erfolgreich angegriffen wurde.

Datenschutzrechtliche Bewertung zur Exchange-Sicherheitsproblematik
Viele Unternehmen sind verunsichert, inwieweit der eigene Betrieb gefährdet ist und personenbezogene Daten tatsächlich abgegriffen worden sind. Während zu Beginn laut Microsoft primär Forschungseinrichtungen mit Pandemie-Fokus, Hochschulen, Anwaltsfirmen und Organisationen aus dem Rüstungssektor angegriffen wurden, steht mittlerweile die Annahme im Raum, dass Angriffe branchenunabhängig erfolgen.

Unabhängig von einer genaueren Bewertung eines möglichen datenschutzrechtlichen Schadens einer Cyberattacke sind Verantwortliche mit gefährdeten Systemen zunächst verpflichtet, umgehend die bereitgestellten Patches für ihre Systeme zu installieren und damit ihrer Verpflichtung gemäß Art. 32 DS-GVO nachzukommen, die Sicherheit ihrer Verarbeitungstätigkeiten zu gewährleisten. Verantwortliche, die dieser Aufgabe bislang nicht nachgekommen sind, trifft angesichts des auch durch die zentrale Funktion von Exchange Servern im Kommunikationssystem der Unternehmen außerordentlich erhöhten Sicherheitsrisikos unabhängig von weiteren Befunden die Verpflichtung, die Sicherheitslücke als Schutzverletzung binnen 72 Stunden zu melden. Dies stellt sicher, dass die weiteren Schritte zur Wiederherstellung der Sicherheit des Gesamtsystems unter Aufsicht des BayLDA durchgeführt werden.

Angesichts des hohen Schadenspotentials bei Ausnutzung der Sicherheitslücke und der deutlich erhöhten Wahrscheinlichkeit solcher Angriffe bestehen auch für Verantwortliche, die das erforderliche Update bereits zeitnah durchgeführt haben, noch weitere Untersuchungspflichten: Um auszuschließen, dass ein Einspielen der Microsoft-Updates zu spät gelungen ist und zwischenzeitlich Schadcode installiert wurde, sind sämtliche betroffenen Systeme dahingehend zu überprüfen, ob sie noch den Anforderungen des Art. 32 DS-GVO gebotenen Schutz gewährleisten. Treten dabei Schutzverletzungen, etwa sogenannte Hintertüren im System auf, ist in diesen Fällen ebenfalls eine Meldung an die Datenschutzaufsichtsbehörde durchzuführen, da dann für die betroffenen Personen ein Risiko besteht.

Inwieweit in manchen Fällen sogar ein hohes Risiko für betroffene Personen besteht und eine Benachrichtigung derer nach Art. 34 DS-GVO notwendig ist, ist letztendlich abhängig vom Einzelfall. Hier ist eine Individualprüfung durch den eigenen Datenschutzbeauftragten der Unternehmen erforderlich.

Datenschutzprüfung des BayLDA in Bayern
Seit der Presseinformation des BSI vergangene Woche erhält das BayLDA Beratungsanfragen und Meldungen zu Datenschutzverletzungen von verschiedenen Unternehmen. Daher hat das BayLDA die Prüfkapazitäten des eigenen Cyberlabors eingesetzt, um betroffene bayerische Unternehmen auf die akute Gefährdungslage hinzuweisen. Eines der Ziele der Prüfung ist es, anfällige Exchange Server in Bayern zu identifizieren und deren Betreiber zu kontaktieren.

Das BayLDA hat dafür in einem ersten Prüflauf am 08.03.2021 stichprobenartig 16.502 bayerische Systeme auf ihre mögliche Verwundbarkeit untersucht. Bei den Organisationen, die auf eine Microsoft Exchange-Kommunikationsstruktur setzen, wurde kontrolliert, ob der notwendige Patch-Level zum Schließen der Lücken vorhanden ist. Bereits im ersten Prüflauf wurde eine dreistellige Zahl potentiell verwundbarer Server identifiziert, deren Verantwortliche nun umgehend über die datenschutzrechtlichen Verpflichtungen und Konsequenzen unterrichtet werden.

Aufgrund der Vielzahl an betroffenen Firmen kann im Regelfall keine Individualberatung stattfinden. Deshalb etabliert das BayLDA einen Frage-und-Antwort-Bereich (FAQ) auf seiner Website für Unternehmen, die zu diesem Thema Datenschutzfragen haben. Dieser ist unter folgender Adresse erreichbar: www.lda.bayern.de/exchange

Das BayLDA beabsichtigt nach der ersten Information der Unternehmen weitere Prüfläufe. Bei Verstößen gegen die Vorgaben der Datenschutz-Grundverordnung drohen dann den Verantwortlichen, die nicht angemessen reagieren, aufsichtliche Verfahren bis hin zu Geldbußen.

Michael Will
Präsident des Bayerischen Landesamts für Datenschutzaufsicht

Weitere Links:

- BSI Presseinformation: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/210305_Exchange-Schwachstelle.html
- BSI Cyber-Sicherheitswarnung: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-197772-1132.pdf?__blob=publicationFile&v=8
- Microsoft Security Information „HAFNIUM targeting Exchange Servers with 0-day exploits“ https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
- BayLDA Patch Management Checkliste: https://www.lda.bayern.de/media/checkliste/baylda_checkliste_patch_mgmt.pdf

---