Microsoft Exchange-Server: Handlungsbedarf für Unternehmen

10. März 2021 von David Vasella

Vor einigen Tagen wurde bekannt, dass Microsoft Exchange E-Mail-Server von Schwachstellen betroffen sind (vgl. z.B. die Mitteilungen des deutschen BSI). In ihrer Kombination konnten diese Schwachstellen für Angriffe verwendet werden, was offenbar breit erfolgt ist (Krebs on Security):

> At least 30,000 organizations across the United States—including a significant number of small businesses, towns, cities and local governments—have over the past few days been hacked by an unusually aggressive **Chinese cyber espionage unit** that's focused on stealing email from victim organizations, multiple sources tell KrebsOnSecurity. The espionage group is exploiting **four newly-discovered flaws in Microsoft Exchange Server email software**, and has seeded hundreds of thousands of victim organizations worldwide with tools that give the attackers total, remote control over affected systems.

Microsoft hat am 3. März Security-Updates für die betroffenen Versionen der Software bereitgestellt. Ein Risiko besteht offenbar besonders für aus dem Internet erreichbaren Exchange-Server (z.B. via Outlook Web Access), aber auch bei der Nutzung weiterer Dienste.

Das Bayrische Landesamt für Datenschutz hat Handlungsbedarf für Bayrische Unternehmen veröffentlicht und dabei auch eine datenschutzrechtliche Bewertung vorgenommen. Eingeleitet wird sie durch die Feststellung,

> 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

Daher sieht das BayLDA folgende Pflichten der betroffenen Verantwortlichen:

— Die **Installation der Patches** ist nach Art. 32 DSGVO zwingend;

— Verantwortliche, die dies noch nicht gemacht haben, "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";

— auch wenn die Patches eingespielt wurden, "sind sämtliche betroffenen **Systeme dahingehend zu überprüfen**, ob sie noch den Anforderungen des Art. 32 DS-GVO gebotenen Schutz gewährleisten";

— "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".

Zum Abschluss:

> 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.1

Behörden
Datenschutzverletzung, Datensicherheit, Deutschland, DSGVO 32, DSGVO 34, Microsoft

suchen

Gesetzestexte

revDSG ohne Botschaft
revDSG mit Botschaft
revDSG auf Englisch
DSGVO
DSG
VDSG

Ähnliche Beiträge:

Erste Reaktion von Microsoft auf Schrems II und die EDSA-Empfehlungen
BayLDA: neue Checklisten u.a. zu Home Office und Cybersicherheit für medizinische Einrichtungen
BayLDA: Abgaben zur aktuellen Kontrolltätigkeit
BayLDA: Muster für Verzeichnis von Verarbeitungstätigkeiten und Verpflichtung zum Datenschutz
Microsoft vs. USA: Fall abgeschrieben

Anmelden