Statement des DDI
zur MS Exchange Sicherheitslücke

Datum	Version	Bearbeiter	Hinweis
11.03.2021	1.0	J. Burkard(DDI)	

1 Ausgangslage

Nach der aktuellen Presseveröffentlichung des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist eines klar: Die neubekannt gewordenen Schwachstellen in Microsoft Exchange-Mail-Servern betreffen auch eine Vielzahl deutscher Firmen. Viele Unternehmen sind verunsichert, inwieweit der eigene Betrieb gefährdet ist und personenbezogene Daten tatsächlich abgegriffen worden sind. Daraus resultierend stellt sich die Frage, ab wann die Meldung einer „Datenpanne“ nach Artikel 33 DSGVO erfolgen muss. Bereits wenn mein Exchange-Server nach Bekanntwerden der Lücke weiter eine gewisse Zeit ohne Sicherheitspatch blieb, man Schadsoftware auf dem Server gefunden hat oder tatsächliche Erkenntnisse vorliegen, dass personenbezogene Daten abgeflossen sind.

2 Bewertung

In den letzten beiden Tagen wurden von einigen Landesdatenschutz-Aufsichtsbehörden Meldungen herausgegeben, wie man dort die Situation bewertet. Leider ergibt sich, wie so oft, kein wirklich einheitliches Vorgehensmodell. Wertet eine Aufsicht bereits die Tatsache, dass erst nach dem 9. März eingespielte Sicherheitspatches bereits als Datenpanne zu sehen ist, gehen andere bereits mit dem Einspieldatum 5. März ins Rennen. Andere sehen erst die Tatsache, dass der ungeschützte Server auch wirklich kompromittiert wurde als Auslöser einer Meldung. Relativ einig ist man sich aber, dass schon das Entdecken der Schadsoftware auf dem Server auch ohne Kenntnisse, ob und welche Daten darüber abgeflossen sind, bereits ein meldepflichtiger Vorgang ist.
Darüber hinaus besteht Konsens, dass die genaue Analyse über abgeflossene Daten notwendig ist und bei einem hohen Risiko für die Betroffenen diese direkt und zeitnah zu informieren sind.

3 Empfehlung des DDI Datenschutz-Teams

Das DDI empfiehlt eine Einzelprüfung bezüglich der Situation Ihrer Systeme und des Bundeslandes, um ein individuelles Vorgehen abzustimmen.

Auf der sicheren Seite sind Sie, falls Schadsoftware auf dem Server entdeckt oder erst nach dem 5. März der Sicherheitspatch eingespielt wurde, wenn eine Meldung nach Artikel 33 DSGVO bei der für Sie zuständigen Aufsicht eingereicht wird.

Eine etwaige Information an Betroffene empfehlen wir erst, wenn gesicherte Erkenntnisse zu den kompromittierten Daten vorliegen.