Sicherheitslücke in MS Exchange Server gibt Anlass zu Prüfungen auf sachgerechte Beseitigung und den Umgang mit den Folgen

Dortmund, 13.09.2021: Das Katholische Datenschutzzentrum konnte jetzt eine im April 2021 begonnene Prüfung abschließen. Dabei wurden eine Reihe von Einrichtungen einer Befragung unterzogen, mit der die sachgerechte Beseitigung einer Sicherheitslücke in Microsoft Exchange Servern und der Umgang mit eventuellen Folgen untersucht werden sollte. Als Teilnehmer der Prüfung wurden Einrichtungen ausgewählt, bei denen der Einsatz dieser Software bekannt war oder vermutet wurde.

Im Februar 2021 musste Microsoft eine schwere Sicherheitslücke in dem weitverbreiteten E-Mail-Serverprogramm „Exchange Server“ einräumen. Hintergrund: Der Server bietet die Möglichkeit, über das https-Protokoll und den Port 443 auf die Postfächer auch dann zuzugreifen, wenn der Anwender kein Client-Programm (etwa MS Outlook) verwendet, sondern nur einen Webbrowser zur Verfügung hat. Genau über diesen Weg war es aber lange Zeit auch möglich, unberechtigten Zugriff auf die Daten des Servers zu nehmen und dadurch etwa Daten und Adressen von E-Mails auszulesen oder Schadsoftware auf dem Server zu platzieren.

Alle Betreiber von MS Exchange Server standen vor der Aufgabe, nach dem Bekanntwerden der Sicherheitslücke diese Lücke schnellstens durch Einspielen eines Updates („Sicherheitspatch“) zu schließen und ihre Systeme darauf hin zu untersuchen, ob die Sicherheitslücke bereits ausgenutzt worden war, also nachweislich Schadsoftware installiert wurde oder sogar bereits Daten abgeflossen waren.

Das Katholische Datenschutzzentrum hat daher einige Einrichtungen im Rahmen einer Prüfung über den Umgang mit der Sicherheitslücke und deren eventuellen Folgen befragt.

In einem ersten Schritt wurden durch das Katholische Datenschutzzentrum die öffentlich verfügbaren Informationen der E-Mail-Server der Einrichtungen abgefragt. So konnte auch erkannt werden, ob die Sicherheitslücke noch besteht. Positiv festzustellen ist, dass zum Zeitpunkt der Abfrage die Sicherheitslücke bei allen geprüften Einrichtungen bereits geschlossen war.

Im zweiten Schritt wurden den zu prüfenden Einrichtungen die ermittelten Informationen mitgeteilt und die Verantwortlichen gebeten, das Vorgehen beim Schließen der Sicherheitslücke zu beschreiben und darzulegen, wie geprüft worden war, dass die Sicherheitslücke nicht schon vor der Behebung der Schwachstelle ausgenutzt worden war und was als weiterer Umgang mit eventuellen Folgen geplant ist (etwa das Beobachten eventueller ungewöhnlicher Datenströme als Anzeichen einer unberechtigten Datenübertragung durch Schadsoftware).

Die Antworten der angeschriebenen Einrichtungen zeigten durchweg ein angemessenes und professionelles Verhalten der Verantwortlichen. In einigen Fällen hatte der Vorfall dazu geführt, dass der Serverbetrieb an einen professionellen Dienstleister abgegeben wurde oder kleine Einrichtungen sich der IT-Struktur von übergeordneten Verbünden angeschlossen haben. In keinem Fall musste eine Anordnung ausgesprochen werden.

Das Katholische Datenschutzzentrum kann vor dem Hintergrund des Ergebnisses der Prüfung ein positives Fazit ziehen, da die geprüften Einrichtungen schnell reagiert und die Sicherheitslücke beseitigt haben.