Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz

Neue Welle von Schadsoftware – Anstieg von Datenpannen in diesen Tagen aufgrund von Phishing Mails

In den ersten Tagen des Juni 2020 sind zahlreiche Organisationen und Betriebe in Rheinland-Pfalz mit einer neuartigen Schadsoftware vergleichbar der Schadsoftware Emotet infiziert worden.

Beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI) sind seit dem 20. Mai acht entsprechende Datenpannen gemeldet worden. Es sind Unternehmen als auch öffentliche Stellen von den Angriffen betroffen. Bei der derzeitigen Angriffswelle handelt es sich um eine Schadsoftware, bei der der Schädling in der Regel neben den E-Mail-Kontakten auch die vorhandene E-Mail-Kommunikation ausliest und sich dann auf dem E-Mail-Weg weiterverbreitet. Ist die Schadsoftware erstmal in IT-Systeme eingedrungen, kann sie unter Umständen andere Schadprogramme nachladen.

Ob und gegebenenfalls in welchem Umfang bei den jüngsten Angriffen in Rheinland-Pfalz über die Daten aus der E-Mail-Kommunikation hinaus weitere Daten abgefließen sind, ist derzeit noch offen. Nach den ersten Angaben der Verantwortlichen der betroffenen Unternehmen und Einrichtungen sind bisher keine weiteren Abflüsse von Daten festgestellt worden; dies ist jedoch Gegenstand weiterer Ermittlungen. Datenschutzrechtlich sind Angriffe mit der neuartigen Schadsoftware problematisch, weil durch den Abfluss der E-Mails personenbezogene Daten unbefugten Dritten bekannt werden. Diese E-Mails können, je nach Zusammenhang, sensible Daten der Absender enthalten.

Die Angriffe verlaufen in der Regel nach folgendem Muster: Die Schadsoftware liest Kontaktbeziehungen und E-Mail-Inhalte aus den Postfächern bereits infizierter Systeme aus. Anschließend werden authentisch aussehende Spam-Mails an die Empfänger aus der Kontaktliste verschickt. Diese erhalten also fingierte Mails von Absendern, mit denen sie kürzlich tatsächlich in Kontakt standen, was das Risiko erhöht, dass den E-Mails Vertrauen entgegengebracht wird. Die Beschreibungen der Betroffenen in Rheinland-Pfalz in den vergangenen Tagen ähneln sich in diesem Sinne: E-Mails mit den Adressen der betroffenen Unternehmen und Einrichtungen sind an Personen gegangen, die aus zwei Elementen bestanden. Im oberen Teil der E-Mail war ein

kurzer Satz mit einem Link enthalten, über den womöglich eine Infektion erfolgen könnte. Im unteren Teil der E-Mail war eine ältere E-Mail angehängt, die die Person zuvor an das Unternehmen oder die Einrichtung gesandt hatte.

Bei einem Befall mit der neuartigen Schadsoftware liegt datenschutzrechtlich eine Datenschutzverletzung vor, die nach Artikel 33 DS-GVO bei der zuständigen Aufsichtsbehörde innerhalb von 72 Stunden zu melden ist. Nach einem Angriff sollten alle betroffenen Personen, das heißt alle E-Mail-Absender, die sich im Postfach des infizierten Unternehmens befinden, nach dem Motto „Sharing is caring“ (Vorbeugen durch Informationen teilen) über den Vorfall informiert werden, um eine Ausbreitung zu verhindern. Handelt es sich bei den betroffenen E-Mails um E-Mails mit sensiblen Inhalten wie besonders geschützte Daten nach Art. 9 DS-GVO, ist von einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen auszugehen. In diesen Fällen unterliegt der Verantwortliche einer Pflicht zur Benachrichtigung der betroffenen Personen nach Art. 34 Abs. 1 DS-GVO.

Der LfDI empfiehlt den betroffenen Unternehmen und Organisationen ihre Mitarbeiter für die neue Welle von Phishing-Mails zu sensibilisieren und die Sicherheitsvorkehrung des Bundesamts für Sicherheit in der Informationstechnik zur Vorbeugung eines Angriffs zu befolgen. Weitere Informationen gibt es beim Bundesamt und dem Bayerischen Landesamt für Datenschutzaufsicht.

Der Bayerische Landesbeauftragte für den Datenschutz und das Bayerische Landesamt für Datenschutzaufsicht stellen eine Checkliste mit Best-Practice-Maßnahmen zur Sicherstellung der Verfügbarkeit bezüglich Cyberattacken in medizinischen Einrichtungen¹ zur Verfügung.

Prof. Dr. Dieter Kugelmann, LfDI Rheinland-Pfalz

¹ https://www.datenschutz-bayern.de/presse/20200603_Best_Practice_Med.html