Der Bayerische Landesbeauftragte
für den Datenschutz

Meldung nach Art. 33 Datenschutz-Grundverordnung bei Hackerangriff

Aktuelle Kurz-Information 58

Stichwörter: Datensicherheitsverletzung, Meldepflicht (Art. 33 DSGVO) – Hackerangriff, Meldung (Art. 33 DSGVO) – Meldung (Art. 33 DSGVO), Hackerangriff | **Stand:** 1. Februar 2025

Was sind die Kernaussagen dieser Aktuellen Kurz-Information?

- Hackerangriffe auf bayerische öffentliche Stellen lösen regelmäßig die Meldepflicht nach Art. 33 DSGVO aus.
- Bayerische öffentliche Stellen müssen auch aktiv werden, wenn der Hackerangriff „nur" den eigenen Auftragsverarbeiter betrifft.
- Die Meldepflicht darf „abschichtend" erfüllt werden.

Kein Verantwortlicher wünscht sich einen Hackerangriff. Dennoch kommen solche Angriffe nach meinen Erfahrungen immer öfter auch bei bayerischen öffentlichen Stellen und ihren IT-Dienstleistern vor. Hackerangriffe kosten Geld und Nerven, wenn personenbezogene Daten betroffen sind, auch schnell Vertrauen. Besonders wichtig ist daher gute Prävention und Absicherung der IT-Systeme. Am besten „fährt" der Verantwortliche, der die Routinen für den Fall eines Hackerangriffs stets aktuell verfügbar hat – und dann nie benötigt. 1

Das vorliegende Papier befasst sich mit einem Aspekt dieser Routinen, nämlich der Meldepflicht für Datensicherheitsverletzungen nach Art. 33 Datenschutz-Grundverordnung (DSGVO). Herausgegriffen sind dabei einige Punkte, die in meiner Prüfungs- und Beratungspraxis immer wieder Anlass zu (Nach-)Fragen gegeben haben. 2

1. Ausgangssituation

In letzter Zeit nehmen Angriffe auf die IT-Infrastruktur bayerischer öffentlicher Stellen und ihrer IT-Dienstleister stark zu. Betroffen sind insbesondere Krankenhäuser, Gemeinden, Landratsämter und Hochschulen. Die möglichen Folgen solcher Angriffe sind vielfältig; sie reichen von Datenabfluss und Datenverschlüsselung über andere Störungen der Verfügbarkeit bis hin zu mehrwöchigen Systemabschaltungen. Viele Stellen haben offenbar immer noch die Hoffnung, sie wären zu klein oder für Angreifer gänzlich uninteressant. Gerade umfassende Angriffe auf bekannte Sicherheitslücken zeigen jedoch, dass diese Hoffnung trügerisch ist. 3

Obwohl die Mehrzahl der Angriffsversuche von der Sicherheitsinfrastruktur der öffentlichen Stellen – etwa von Firewalls oder Systemen zur Angriffserkennung – abgewehrt werden kann, kommt es auch immer wieder zu erfolgreichen Angriffen, in deren Verlauf ein Hacker die Kontrolle über IT-Komponenten, im schlimmsten Fall gar einen Zugriff auf personenbezogene Daten erlangt. In diesem Sinn erfolgreich ist ein Angriff insbesondere dann, wenn der Hacker 4

- personenbezogene Datenbestände verschlüsseln, verändern, löschen oder abziehen konnte und/oder

Der Bayerische Landesbeauftragte für den Datenschutz
80538 München | Wagmüllerstraße 18 | Telefon: +49 89 21 26 72-0
poststelle@datenschutz-bayern.de | https://www.datenschutz-bayern.de

– Zugriff auf eine Administrator-Kennung oder Zugang zu einer IT-Komponente im internen Netz (zum Beispiel Storage-Systeme, Backup-Systeme, virtuelle Server/Hypervisor) erlangen konnte und ein Zugriff auf Bestände personenbezogener Daten nicht zweifelsfrei ausgeschlossen werden kann.

5 Zudem kann – ohne Vorliegen eines Hackerangriffs – der Fall eintreten, dass über das Internet aufgrund von Sicherheitslücken oder Fehlkonfigurationen personenbezogene Daten für Unbefugte zugänglich sind. Auch hier ist grundsätzlich anzunehmen, dass es zu unbefugten Zugriffen gekommen ist, wenn dies nicht beispielsweise anhand einer Protokollierung zweifelsfrei ausgeschlossen werden kann.

6 In diesen Fällen ist stets zu prüfen, ob eine Meldung nach Art. 33 DSGVO erforderlich ist; in aller Regel werden die Voraussetzungen erfüllt sein. Die Vorgehensweise bei einer solchen Prüfung sowie bei der Erfüllung der Meldepflicht erläutert eine Orientierungshilfe, die auf meiner Homepage bereitgestellt ist.[1]

2. Insbesondere: Angriff bei IT-Dienstleister

7 Bayerische öffentliche Stellen lagern den IT-Betrieb oftmals ganz oder in Teilen an IT-Dienstleister aus. Leider hat sich in der Vergangenheit gezeigt, dass auch solche IT-Dienstleister von erfolgreichen Hackerangriffen betroffen sein können. Vielerorts besteht die Auffassung, die Bearbeitung eines derartigen Sicherheitsvorfalls und damit auch die Erfüllung der Meldepflicht nach Art. 33 DSGVO sei allein Aufgabe des IT-Dienstleisters. Dies trifft jedoch nur für dessen eigene (!) Daten zu, nicht für die Daten des Auftraggebers, für den der IT-Dienstleister – meist im Rahmen eines Auftragsverarbeitungsverhältnisses – tätig wird.

8 Dies bedeutet allerdings auch, dass bei Hackerangriffen oder sonstigen Sicherheitsvorfällen die bayerische öffentliche Stelle als Auftraggeber Verantwortlicher im Sinne der Datenschutz-Grundverordnung bleibt, auch wenn sich der Vorfall – rein praktisch betrachtet – in der Sphäre des IT-Dienstleisters abspielt. Daran ändert sich selbst dann nichts, wenn der Auftragsverarbeiter den Hackerangriff erleichtert hat, weil er beispielsweise Sicherheitsupdates nicht rechtzeitig eingespielt hat. Hier zeigt sich wieder einmal, wie wichtig eine sorgfältige Auswahl und auch eine regelmäßige Kontrolle von IT-Dienstleistern ist; Einzelheiten habe ich in einem Leitfaden erläutert, der auf meiner Homepage abrufbar ist.[2]

9 Der Auftragsverarbeiter muss im Fall eines Hackerangriffs grundsätzlich seinen Auftraggeber verständigen. Der Auftraggeber muss dann die Meldepflicht nach Art. 33 DSGVO erfüllen. Hierbei genügt es nicht, allgemeine Informationsschreiben des Dienstleisters an die Datenschutz-Aufsichtsbehörde „durchzureichen“. Der Auftraggeber muss den Vorfall vielmehr eigenständig bewerten und insbesondere für die eigenen betroffenen Daten eine Risikoanalyse durchführen.

10 Ein „vorsorgender“ Auftraggeber wird diese Aspekte bereits bei der Beschaffung einer IT-Dienstleistung berücksichtigen: Es spricht nichts dagegen, mit dem Auftragsverarbeiter eine Verpflichtung zu vereinbaren, im Fall eines Hackerangriffs die für eine Meldung nach Art. 33 DSGVO nötigen Informationen bereitzustellen – soweit erforderlich unter Einschluss einer den einschlägigen Standards entsprechenden Risikoanalyse.

3. Empfehlungen für die Erfüllung der Meldepflicht nach Art. 33 DSGVO im Fall eines Hackerangriffs

Auf einen Hackerangriff folgt – wie auch auf manch anderen Sicherheitsvorfall – oftmals eine längere Phase der „Sachverhaltserhärtung", die in der Regel forensische Analysen und polizeiliche Ermittlungen einschließt. Auch das Wiederaufsetzen der betroffenen IT-Systeme und die Implementierung geeigneter technisch-organisatorischer Maßnahmen kosten Zeit. 11

Vor diesem Hintergrund ist auch für die Erfüllung der Meldepflicht nach Art. 33 DSGVO ein „abschichtendes" Vorgehen sinnvoll: 12

Erstmeldung innerhalb von 72 Stunden

Wenn nach einer komplexen Datensicherheitsverletzung Risiken für die Rechte und Freiheiten der betroffenen Personen nicht zweifelsfrei ausgeschlossen werden können, ist eine Meldung nach Art. 33 DSGVO angezeigt. In der Meldung sind alle bisher bekannten Tatsachen zum Angriff oder Sicherheitsvorfall aufzuführen. Insbesondere sollte eine erste Einschätzung zur Sensibilität der Daten und zur Anzahl der betroffenen Personen abgegeben werden. Zudem sollten bereits Angaben gemacht werden, ob eine Information der betroffenen Personen gemäß Art. 34 DSGVO vorgesehen oder schon erfolgt ist. 13

Zwischenberichte alle zwei Wochen

Die Meldepflicht nach Art. 33 DSGVO ist erst erfüllt, wenn der Datenschutz-Aufsichtsbehörde alle gesetzlich geforderten, im Online-Meldeformular[3] strukturierten Angaben übermittelt sind. Bei längerem Klärungsbedarf und anzunehmender Betroffenheit von besonders sensiblen personenbezogenen Daten – insbesondere nach Art. 9 Abs. 1 DSGVO – ist es zweckmäßig, unaufgefordert alle zwei Wochen einen kurzen schriftlichen Zwischenbericht zu den wichtigsten Punkten zu erstatten. Dies betrifft insbesondere Krankenhäuser und andere medizinische Einrichtungen. 14

Abschlussbericht nach Aufklärung des Hackerangriffs oder sonstigen Sicherheitsvorfalls

Spätestens nach der internen Aufklärung des Vorfalls ist ein Abschlussbericht erforderlich – sei es mit dem Ergebnis, dass kein Zugriff auf personenbezogene Daten erfolgte und somit keine Risiken bestanden, sei es mit folgenden Informationen und Unterlagen: 15

- endgültige Anzahl der betroffenen Personen und Kategorien von personenbezogenen Daten;
- konkrete Risikoanalyse hinsichtlich der betroffenen Daten;
- forensischer Abschlussbericht, insbesondere zur Ursache des Vorfalls und zur Möglichkeit eines Datenabflusses;
- Ermittlungsergebnisse der zuständigen Polizeidienststelle (soweit vorhanden);

- Ergebnisse einer Darknet-Recherche, wenn ein Datenabfluss festgestellt wurde, oder Begründung, warum keine Darknet-Recherche durchgeführt wurde;
- Erläuterung der ergriffenen und geplanten Maßnahmen beim Verantwortlichen und einem gegebenenfalls beauftragten IT-Dienstleister;
- Angaben zur Erfüllung einer Benachrichtigungspflicht nach Art. 34 DSGVO mit Kopie eines entsprechenden Informationsschreibens (soweit erforderlich).

4. Folgen von Defiziten bei der Erfüllung der Meldepflicht nach Art. 33 DSGVO

Defizite bei der Erfüllung der Meldepflicht nach Art. 33 DSGVO können Anlass für eine Beanstandung (Art. 16 Abs. 4 Satz 1 Bayerisches Datenschutzgesetz – BayDSG) oder eine Verwarnung (Art. 58 Abs. 2 Buchst. b DSGVO) sein; im Einzelfall kann auch die Anordnung einer Verarbeitungsbeschränkung oder eines Verarbeitungsverbots (Art. 58 Abs. 2 Buchst. f DSGVO) in Betracht kommen – etwa dann, wenn wiederholte Datenschutzverletzungen belegen, dass der Verantwortliche nicht in der Lage ist, eine sichere Verarbeitung der betroffenen personenbezogenen Daten zu gewährleisten. Bezieht sich die Pflichtverletzung auf eine Tätigkeit, mit der die öffentliche Stelle am Wettbewerb teilnimmt, kann auch eine Geldbuße (Art. 83 Abs. 4 Buchst. a DSGVO) verhängt werden. Das Ernstnehmen der Meldepflicht nach Art. 33 DSGVO lohnt also.

[1] Bayerischer Landesbeauftragter für den Datenschutz, Meldepflicht und Benachrichtigungspflicht des Verantwortlichen, Stand 6/2019, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

[2] Bayerischer Landesbeauftragter für den Datenschutz, Leitfaden zum Outsourcing kommunaler IT, Stand 3/2021, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

[3] Internet: https://www.datenschutz-bayern.de/service/data_breach.html.