Der Bayerische Landesbeauftragte
für den Datenschutz

# Strafanzeige als technisch-organisatorische Maßnahme nach Hackerangriff?

## Aktuelle Kurz-Information 57

**Stichwörter:** Datenpanne, Strafanzeige – Hackerangriff, Strafanzeige – Meldepflicht und Strafanzeige – Strafanzeige bei Hackerangriff – Strafanzeige und Meldepflicht | **Stand:** 1. März 2025

**Was sind die Kernaussagen dieser Aktuellen Kurz-Information?**

- Verantwortliche sollten bei einer Datenpanne auch an Mitteilungspflichten denken, die außerhalb der Datenschutz-Grundverordnung geregelt sind.
- Eine Strafanzeige ist im Fall eines Hackerangriffs grundsätzlich eine sinnvolle technisch-organisatorische Maßnahme des Verantwortlichen.

Öffentliche Stellen sind nach Art. 33 Datenschutz-Grundverordnung (DSGVO) verpflichtet, Datensicherheitsverletzungen zu melden, wenn diese ein Risiko für die Rechte und Freiheiten natürlicher Personen darstellen. Dies gilt insbesondere in Fällen von Hackerangriffen, bei denen personenbezogene Daten betroffen sein können. Die Meldung an die zuständige Datenschutz-Aufsichtsbehörde muss unverzüglich und, sofern möglich, innerhalb von 72 Stunden nach Bekanntwerden des Vorfalls erfolgen. 1

Die Meldepflicht dient dazu, Transparenz über den Vorfall zu schaffen und sicherzustellen, dass geeignete Maßnahmen ergriffen werden, um die betroffenen Personen zu schützen und den Schaden zu begrenzen. Dabei sind unter anderem die Art des Angriffs, der Umfang der betroffenen Daten und die möglichen Folgen darzulegen. 2

Es besteht jedoch grundsätzlich keine gesetzliche Verpflichtung, nach Art. 33 DSGVO meldepflichtige Vorfälle auch den Strafverfolgungsbehörden mitzuteilen. Dies führt in der Praxis nicht selten dazu, dass eine Strafanzeige unterbleibt. 3

## 1. Gesetzliche Mitteilungspflichten

Neben der Meldepflicht nach Art. 33 DSGVO können weitere Mitteilungspflichten eingreifen. So müssen Sozialleistungsträger und einige weitere in § 35 Erstes Buch Sozialgesetzbuch genannte Stellen nach § 83a Zehntes Buch Sozialgesetzbuch (SGB X) eine Verletzung des Schutzes von Sozialdaten auch der zuständigen Rechts- oder Fachaufsichtsbehörde melden.[1] Betreiber kritischer Infrastrukturen sowie von Energieversorgungsnetzen und von bestimmten Energieanlagen trifft eine Pflicht zur Meldung an das Bundesamt für Sicherheit in der Informationstechnik, wenn bestimmte Störungen auftreten (§ 8b Abs. 4 BSI-Gesetz – BSIG – und § 11 Abs. 1c Energiewirtschaftsgesetz – EnWG).[2] Staatliche und sonstige an das bayerische Behördennetz angeschlossene Stellen müssen nach Art. 43 Abs. 3 Satz 1 Bayerisches Digitalgesetz (BayDiG) das Landesamt für Sicherheit in der Informationstechnik und ihre jeweilige oberste Dienstbehörde unterrichten, wenn Informationen bekannt werden, die zur Abwehr von Gefahren für die Sicherheit in der Informationstechnik von Bedeutung sind. 4

**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**

5 **Hinweis:** Die „jeweilige oberste Dienstbehörde“ ist bei nachgeordneten staatlichen Stellen das im Behördenaufbau übergeordnete Staatsministerium. Erfüllen Stellen – wie etwa die Regierungen – Aufgaben aus mehreren Geschäftsbereichen, dürfte es darauf ankommen, mit welcher dieser Aufgaben der meldepflichtige Vorfall in Zusammenhang steht. Bei nicht staatlichen Stellen dürfte als oberste Dienstbehörde im vorliegenden Sinne das Staatsministerium anzusehen sein, das die Aufgabe der obersten Aufsichtsbehörde wahrnimmt; jedenfalls legt der systematische Zusammenhang mit Art. 43 Abs. 2 BayDiG nahe, die oberste Dienstbehörde hier nicht entsprechend Art. 2 Satz 1, Art. 136 Bayerisches Beamtengesetz zu bestimmen.

6 Die Strafprozeßordnung sieht ein Recht zur Strafanzeige vor;[3] eine allgemeine, jeden treffende „Anzeigepflicht“ für strafrechtlich relevante Vorgänge besteht demgegenüber grundsätzlich nicht. Zu beachten sind in diesem Zusammenhang aber insbesondere zwei Punkte:

- Bestimmte **Amtsträger** sind zu einer Strafanzeige verpflichtet, wenn ihnen (jedenfalls) in dienstlicher Eigenschaft der Anfangsverdacht einer Straftat bekannt wird. Dies gilt etwa für Polizeibeamte oder Staatsanwälte.[4] Meldepflichtige Datensicherheitsverletzungen im Bereich der Bayerischen Polizei sowie der Staatsanwaltschaften dürften daher regelmäßig eine Strafanzeige oder die Einleitung eines Ermittlungsverfahrens veranlassen.

- § 138 Abs. 1 Strafgesetzbuch (StGB) stellt ausnahmsweise die „Nichtanzeige“ ausgewählter, besonders schwerwiegender Straftaten unter eine Strafdrohung. Die Vorschrift zielt auf eine Abwendung der Bezugstat oder ihrer Folgen.[5] Sie begründet indirekt eine Pflicht zur Strafanzeige für **jedermann**, also auch für Beschäftigte bayerischer öffentlicher Stellen, die von einer Bezugstat gegen ihren Dienstherrn oder Arbeitgeber erfahren. Richtet sich ein Hackerangriff darauf, Staatsgeheimnisse zu erlangen oder auf IT-Infrastruktur einzuwirken, die für einen sicheren Bahn-, Straßen-, Schiffs- oder Luftverkehr erforderlich ist, sollte eine Pflicht zur Strafanzeige nach § 138 Abs. 1 StGB bedacht werden.

  **Beispiel:** Ein Beschäftigter einer IT-Stelle, welche die Verkehrszentrale einer bayerischen Großstadt betreut, stellt fest, dass externe Nichtberechtigte versuchen, Kontrolle über die zentral gesteuerten Lichtzeichenanlagen zu erlangen. – Soweit eine Bezugstat nach § 315 Abs. 3 StGB im Raum steht, sollte der Beschäftigte einen Vorgesetzten informieren, der für den Verantwortlichen als „Bedrohten“ (§ 138 Abs. 1 StGB) handeln darf.

7 Die angesprochenen Mitteilungspflichten unterscheiden sich hinsichtlich ihrer Zielrichtung, der zuständigen Stellen und der konkreten Anforderungen. Während datenschutzrechtliche Meldepflichten den Schutz personenbezogener Daten in den Vordergrund stellen, zielen die Meldepflichten nach dem BSI-Gesetz zunächst einmal auf den Schutz der Infrastruktur ab. Alle Pflichten dienen jedoch dem Schutz bestimmter Rechtsgüter, sollen Transparenz schaffen und effektive Gegenmaßnahmen ermöglichen.

| Rechtsgrundlage | Zuständige Stelle | Mitteilungspflichtiger Vorfall |
|---|---|---|
| Art. 33 DSGVO | Datenschutz-Aufsichtsbehörde | Verletzungen des Schutzes personenbezogener Daten |
| § 83a SGB X | Rechts- oder Fachaufsichts-behörde | Verletzungen des Schutzes von Sozialdaten |
| § 8b Abs. 4 BSIG | Bundesamt für Sicherheit in der Informationstechnik | Störungen bei Betreibern kritischer Infrastruktur |
| § 11 Abs. 1c EnWG | Bundesamt für Sicherheit in der Informationstechnik | Störungen bei Betreibern von Energieversorgungs-netzen und von bestimmten Energieanlagen |
| Art. 43 Abs. 3 Satz 1 BayDiG | Landesamt für Sicherheit in der Informationstechnik und oberste Dienstbehörde | Bekanntwerden von Informationen, die zur Abwehr von Gefahren für die Sicherheit in der Informations-technik von Bedeutung sind |
| § 138 StGB | Strafverfolgungsbehörde, Bedrohter | Vorhaben oder Ausführung bestimmter schwerer Straftaten |

## 2. Rolle der Datenschutz-Aufsichtsbehörden

Die Datenschutz-Aufsichtsbehörden spielen eine zentrale Rolle bei der Kontrolle der Einhaltung der datenschutzrechtlichen Vorgaben, insbesondere im Zusammenhang mit der Datenschutz-Grundverordnung. Sie sind nach Art. 57 Abs. 1 Buchst. a DSGVO verpflichtet, die Anwendung der Datenschutz-Grundverordnung zu überwachen und durchzusetzen. Dabei prüfen und untersuchen sie Datenschutzverstöße, beraten die Verantwortlichen und verhängen geeignete Maßnahmen. 8

Im Falle von Hackerangriffen sind die Datenschutz-Aufsichtsbehörden die ersten Anlaufstellen, um die gesetzlich vorgeschriebenen Meldungen im Hinblick auf den Schutz personenbezogener Daten zu prüfen und sicherzustellen, dass die Verantwortlichen angemessen reagieren. 9

Die Datenschutz-Aufsichtsbehörden können etwa Empfehlungen geben oder Anordnungen treffen, um den Schaden zu begrenzen oder Wiederholungen zu verhindern, wie zum Beispiel die Implementierung technisch-organisatorischer Maßnahmen zur Verbesserung der Datensicherheit. Die Aufgaben der Datenschutz-Aufsichtsbehörden beschränken sich allerdings auf die Anwendung der datenschutzrechtlichen Vorgaben; dementsprechend sind die Befugnisse in Art. 58 Abs. 1 DSGVO auf das Handlungsfeld „Datenschutz“ fokussiert. Zudem stehen hier der Verantwortliche und dessen Handlungsmöglichkeiten im Mittelpunkt. Die Entscheidung, ob eine Strafanzeige erstattet wird, obliegt grundsätzlich erst einmal der betroffenen öffentlichen Stelle. Die Datenschutz-Aufsichtsbehörde kann dem Verantwortlichen diese Entscheidung nicht abnehmen; sie wird oftmals eine Strafanzeige empfehlen und auf die Vorteile eines solchen Vorgehens hinweisen. 10

## 3. Strafanzeige als technisch-organisatorische Maßnahme

11 Im Zusammenhang mit Hackerangriffen kann eine Strafanzeige nämlich eine technisch-organisatorische Maßnahme im Sinn von Art. 32 Abs. 1, Art. 33 Abs. 3 Buchst. d DSGVO darstellen, auch wenn sie nicht durch besondere gesetzliche Regelungen vorgeschrieben ist.

12 Art. 33 Abs. 3 Buchst. d DSGVO verpflichtet Verantwortliche, im Rahmen der Meldung eines Datenschutzvorfalls an die zuständige Datenschutz-Aufsichtsbehörde auch Informationen über ergriffene Maßnahmen zur Minderung der nachteiligen Auswirkungen bereitzustellen. Diese Regelung lässt erkennen, dass Art. 32 Abs. 1 DSGVO im Fall einer Datensicherheitsverletzung konkrete Gegenmaßnahmen des Verantwortlichen fordert. Eine Strafanzeige bei den zuständigen Strafverfolgungsbehörden kann in diesem Kontext eine wirksame Maßnahme sein, die zur Aufklärung und zur Verhinderung weiterer Schäden beiträgt. Möchte eine öffentliche Stelle von einer Strafanzeige absehen, sollte dokumentiert werden, warum diese nicht als mindernde Maßnahme bewertet wurde.

13 Eine Strafanzeige eröffnet die Möglichkeit, über die datenschutzrechtlichen Aspekte hinaus die strafrechtliche Dimension eines Vorfalls zu beleuchten. Dies ist insbesondere dann zweckmäßig, wenn die Angriffsmethoden oder der verursachte Schaden weitreichende Konsequenzen haben. Die Strafanzeige initiiert nämlich Ermittlungen, die darauf abzielen, die Hintergründe und Ursachen des Angriffs zu analysieren. Durch die Zusammenarbeit mit den Ermittlungsbehörden können wichtige Informationen über den Angriff erlangt werden, etwa über die Angreifer und mögliche Schwachstellen in den eigenen Systemen. Dieses Wissen hilft der betroffenen Stelle dabei, die unmittelbaren Auswirkungen zu begrenzen und zukünftige Angriffe besser zu verhindern.

14 Auch liegen bei den Strafverfolgungsbehörden möglicherweise Kenntnisse über die üblichen Vorgehensweisen von Angreifergruppen vor, so dass beispielsweise die Wahrscheinlichkeit eines Datenabflusses oder einer möglicherweise noch folgenden Veröffentlichung von erbeuteten Daten vom Verantwortlichen besser eingeschätzt werden kann. Dies kann auch für die Entscheidung über die Benachrichtigung der von der Verletzung des Schutzes personenbezogener Daten betroffenen Personen nach Art. 34 DSGVO von wesentlicher Bedeutung sein.

15 Darüber hinaus verfügen die Strafverfolgungsbehörden über Werkzeuge und Kompetenzen, um Beweismaterial zu sichern, das für die Analyse und Behebung eines Angriffs entscheidend sein kann. Dies schließt etwa die Identifikation von Schadsoftware, die Rückverfolgung digitaler Spuren und die Analyse der verwendeten Infrastruktur ein. Diese Ergebnisse können dazu beitragen, die Kontrolle über die betroffenen Systeme wiederherzustellen und weiteren Schaden zu verhindern.

16 Weiterhin kann eine Strafanzeige rechtzeitig zu einem Ermittlungserfolg führen, sodass entwendete personenbezogene Daten sichergestellt oder deren weitere Verbreitung verhindert werden können.

17 Auf der organisatorischen Ebene kann eine Strafanzeige zu einer intensiveren Auseinandersetzung mit Sicherheitsprozessen führen und das Bewusstsein der Mitarbeitenden für Cybersicherheitsrisiken verbessern.

## 4. Fazit

Eine Strafanzeige und die Meldung nach Art. 33 DSGVO erfüllen unterschiedliche, aber sich ergänzende Zwecke. Während die Datenschutz-Aufsichtsbehörde die Einhaltung der Datenschutz-Grundverordnung sicherstellt und die Rechte der betroffenen Personen schützt, fokussieren sich die Strafverfolgungsbehörden auf die rechtliche Verfolgung der Täter und die Prävention weiterer Vorfälle. In Ergänzung können beide Maßnahmen dazu beitragen, die möglichen nachteiligen Auswirkungen eines Vorfalls abzumildern. 18

Auch wenn meist keine Pflicht zur Anzeige bei den Strafverfolgungsbehörden besteht, empfehle ich, die Prüfung eines solchen Vorgehens standardmäßig in die internen Prozesse zum „Handling" von Hackerangriffen aufzunehmen. Dadurch kann nicht nur das behördeninterne Niveau von Datenschutz und IT-Sicherheit gehoben, sondern auch behördenübergreifend ein Beitrag zur Bekämpfung von Cyberkriminalität geleistet werden. 19

1 Dazu vertiefend Engelbrecht, Meldepflicht gegenüber der Rechts- oder Fachaufsichtsbehörde bei einer Verletzung des Schutzes von Sozialdaten, NZS 2019, 693.

2 Näher Hessel/Potel, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit, 2023, § 8b BSIG Rn 13 ff. und Voigt/Böhme, a. a. O., § 11 EnWG Rn. 130 ff.

3 § 158 Abs. 1 StPO, dazu Kölbel/Ibold, in: Münchener Kommentar zur Strafprozessordnung, 2. Aufl. 2024, § 158 StPO Rn. 11 f.

4 Näher Weingarten, in: Karlsruher Kommentar zur Strafprozessordnung, 9. Aufl. 2023, § 158 StPO Rn. 25 ff.

5 Sternberg-Lieben, in: Schönke/Schröder, Strafgesetzbuch, 30. Aufl. 2019, § 138 StGB Rn. 1 f.