

Datenpanne und Cyberangriff: Was Unternehmen nach der DSGVO tun müssen

Die Zahl der Cyberangriffe ist durch die technische Entwicklung von KI stark gestiegen. Die Angriffe können nicht nur zu massiven finanziellen Schäden und Betriebsausfällen führen, sondern auch rechtliche Konsequenzen haben, wenn personenbezogene Daten offengelegt oder sogar abgezogen werden.

DATENPANNE ODER CYBERANGRIFF: WIE MÜSSEN UNTERNEHMEN REAGIEREN?

Ein verdächtiger Hinweis bedeutet nicht automatisch, dass ein Unternehmen Opfer eines Hacking-Angriffs geworden ist. Aber es ist wichtig, die Lage ernst zu nehmen und schnell zu handeln.

1. Technische Prüfung einer Datenpanne oder eines Cyberangriffs

Der erste Schritt besteht darin, zu prüfen, ob es tatsächlich einen unbefugten Zugriff gab und welche Systeme von dem Angriff betroffen sind.

Die Einschaltung der eigenen IT und in der Folge ggf. die zügige Beauftragung einer forensischen Untersuchung des Vorfalls durch spezialisierte Dienstleister ist unabdingbar.

Die IT muss schnell handeln und entscheiden, ob betroffene Systeme gegebenenfalls vom Netzwerk getrennt werden, um eine Ausbreitung der Bedrohung zu verhindern.

Nach den ersten Eindämmungsmaßnahmen müssen IT-forensische Untersuchungen die Ursache ermitteln und auch den Umfang der Verletzung bestimmen. Ermittelt werden muss aus datenschutzrechtlicher Sicht die Art des Vorfalls, die Anzahl der betroffenen Personen und Datenkategorien, die Tatsache, ob Daten lediglich eingesehen werden konnten oder ob befürchtet werden muss, dass diese von den Angreifern kopiert wurden. All dies ist detailliert zu dokumentieren. Zudem sind technische Maßnahmen zur Eindämmung zu ergreifen und es müssen Maßnahmen definiert werden, um derartige Vorfälle für die Zukunft so gut wie möglich zu verhindern.

2. Datenpanne nach DSGVO rechtlich prüfen und Risiko bewerten

Nach der DSGVO sind Unternehmen zum Schutz der von ihnen verarbeiteten personenbezogenen Daten verpflichtet.

Der betriebliche Datenschutzbeauftragte ist so früh wie möglich in die Aufarbeitung des Vorfalls einzubeziehen. Sobald erste Ergebnisse der forensischen Untersuchung bereitstehen, sind diese dem Datenschutzbeauftragten zu melden und es muss eine datenschutzrechtliche Bewertung und



Risikoanalyse des Vorfalls durchgeführt werden. Auf Grundlage der Untersuchung ist zu bewerten, welches Risiko für die Rechte und Freiheiten der betroffenen Personen besteht. Dabei sind insbesondere zwei Faktoren entscheidend: die mögliche Schwere des Schadens und die Wahrscheinlichkeit, dass dieser tatsächlich eintritt. Zur Bewertung der Risikostufe kann das DSK-Kurzpapier Nr. 18 „Risiko für die Rechte und Freiheiten natürlicher Personen“ als erste Orientierungshilfe dienen. Die Ergebnisse dieser Bewertung sind anschließend maßgeblich dafür, welche weiteren Maßnahmen getroffen werden müssen.

Im Rahmen der DSGVO-Risikobewertung muss geprüft werden, ob die Datenpanne ein Risiko für die Rechte und Freiheiten der betroffenen Personen begründet und deshalb Melde- oder Informationspflichten bestehen.

Zu beachten ist, dass es sich bei der Bewertung um eine juristische Bewertung handelt, die von Juristen vorgenommen werden sollte, da das Ergebnis weitreichende Folgen für das Unternehmen haben kann.

3. Wann muss eine Datenpanne gemeldet werden?

Liegt eine meldepflichtige Datenpanne vor, besteht nach Art. 33 DSGVO eine Meldepflicht gegenüber der zuständigen Datenschutzbehörde. Die Meldung hat unverzüglich und möglichst innerhalb von 72 Stunden nach Bekanntwerden der Verletzung zu erfolgen. Eine Ausnahme besteht, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt. Hier ist wieder oben beschriebene Risikoeinschätzung maßgeblich.

Neben der Meldung an die Aufsichtsbehörde kann auch eine unmittelbare Benachrichtigung der betroffenen Personen erforderlich sein. Nach Art. 34 DS-GVO besteht diese Pflicht, wenn die Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hat. Die Betroffenen sind in diesem Fall unverzüglich und in klarer und einfacher Sprache über die Art der Verletzung sowie deren mögliche Folgen, die ergriffenen und möglichen Maßnahmen und eine Anlaufstelle für weitere Informationen zu informieren.

4. Cyberangriff: Wann sollten Unternehmen Strafanzeige erstatten?

Zwar ist nicht jeder Hacking-Angriff strafbar, ein frühzeitiges Einschalten der Strafverfolgungsbehörde kann aber bei der weiteren Aufklärung des Vorfalls unterstützen und zur Verhinderung weiterer Schäden beitragen. Im Rahmen der Bewältigung eines Cybervorfalles sind geeignete Maßnahmen zu ergreifen, um mögliche nachteilige Auswirkungen zu begrenzen. Eine Strafanzeige kann eine solche geeignete Maßnahme darstellen.

Darüber hinaus könnte sie für den Versicherungsschutz einer bestehenden Cyberversicherung relevant werden. Mögliche Vorgaben des Versicherers sollten daher frühzeitig geprüft und bei der Entscheidung, ob Strafanzeige zu gestellt werden soll, berücksichtigt werden.



5. Maßnahmen zur Verbesserung der IT-Sicherheit nach einem Cyberangriff

Auf Grundlage der gewonnenen Erkenntnisse sind nach Absprache mit IT-Experten geeignete Sicherheitsmaßnahmen zu ergreifen, um weitere Schäden zu vermeiden und zukünftige Angriffe zu verhindern.

Dazu gehört unter anderem, festgestellte Schwachstellen zu beheben und das Schutzniveau künftigen Gefahren anzupassen, zum Beispiel durch das Einrichten neuer Accounts und Passwörter und die Einführung einer Zwei-Faktor-Authentifizierung. Darüber hinaus sollten Mitarbeiter regelmäßig zum sicheren Umgang mit IT-Systemen und möglichen Sicherheitsrisiken geschult werden. Eine Überwachung der Systeme trägt dazu bei, weitere unbefugte Zugriffe frühzeitig zu erkennen, wobei klare interne Abläufe und Protokolle für den Umgang mit Sicherheitsvorfällen dabei helfen können, in Zukunft schneller und koordiniert auf vergleichbare Vorfälle zu reagieren.

WELCHE IT-SICHERHEITSMAßNAHMEN MÜSSEN UNTERNEHMEN GEGEN CYBERANGRIFFE TREFFEN?

Zu beachten ist hierbei aber auch, dass Unternehmen nicht verpflichtet sind, alle denkbaren Maßnahmen zu ergreifen, um Cyberangriffe zu verhindern. Dies hat das SG Nürnberg erst kürzlich mit Urteil vom 10.06.2026 wieder entschieden.

Demnach ist ein erfolgreicher Hacking-Angriff noch kein Beweis dafür, dass ein Unternehmen seine Daten unzureichend geschützt hat.

Unternehmen sind verpflichtet, in Anbetracht der verarbeiteten Daten, der Art der Verarbeitung und den möglichen Risiken für die Betroffenen geeignete technische und organisatorische Schutzmaßnahmen zu treffen – nicht aber, Angriffe unter allen Umständen zu verhindern.

FAZIT: BEI DATENPANNEN UND CYBERANGRIFFEN SCHNELL UND RECHTSSICHER HANDELN

Bei Verdacht auf eine Datenpanne oder einen Cyberangriff ist Eile geboten. Unternehmen müssen technische Sofortmaßnahmen und die rechtliche Prüfung nach der DSGVO parallel einleiten. Weitere rechtliche Maßnahmen wie Meldungen bei der Aufsichtsbehörde oder Benachrichtigung der Betroffenen müssen sorgfältig geprüft werden. Auch eine Strafanzeige und zu ergreifende weitere Schritte sind zu bewerten und zu koordinieren.

Melden Sie sich, wenn Sie diesbezüglich Hilfe benötigen. Unser Team aus erfahrenen Rechtsanwälten führt Sie Schritt für Schritt durch die rechtlichen Aspekte von Datenschutzverletzungen wie Cyberangriffen oder anderen Vorfällen und hilft Ihnen, rechtliche Risiken so gering wie möglich zu halten.



FAQ

Wann liegt eine Datenpanne im Sinne der DSGVO vor?

Eine Datenpanne ist eine Verletzung des Schutzes personenbezogener Daten. Das ist etwa der Fall, wenn Unbefugte auf Daten zugreifen oder sie einsehen, kopieren, verändern oder löschen. Hacking-Angriffe sind ein typischer Auslöser. Auch verlorene Datenträger, falsch versandte E-Mails oder Fehlkonfigurationen können eine Datenpanne darstellen.

Was ist der erste Schritt bei Verdacht auf einen Cyberangriff?

Zuerst muss technisch geprüft werden, ob es einen unbefugten Zugriff gab und welche Systeme betroffen sind. Schalten Sie sofort die eigene IT ein und beauftragen Sie gegebenenfalls zügig einen spezialisierten IT-Forensik-Dienstleister. Die IT entscheidet auch, ob betroffene Systeme vom Netzwerk getrennt werden müssen, damit sich der Angriff nicht weiter ausbreitet.

Wie sollten Unternehmen nach einem Cyberangriff Beweise sichern?

Eindämmung und Beweissicherung stehen in einem Spannungsfeld. Wer Systeme vorschnell neu aufsetzt oder Logdateien löscht, vernichtet Spuren, die für die Forensik, eine Strafanzeige und die Versicherung benötigt werden. Stimmen Sie die ersten Schritte deshalb mit dem Forensik-Dienstleister ab. Die Beweissicherung gehört von Anfang an dazu.

Was muss die forensische Untersuchung aus Sicht des Datenschutzes klären?

Aus datenschutzrechtlicher Sicht muss sie vor allem Folgendes klären:

- welche Art von Vorfall vorliegt,
- wie viele Personen und welche Datenkategorien betroffen sind,
- ob die Daten nur eingesehen oder möglicherweise auch abgezogen wurden.

Alle Erkenntnisse sind sorgfältig zu dokumentieren. Sie bilden die Grundlage für die rechtliche Bewertung und für mögliche Meldungen.

Wann muss der Datenschutzbeauftragte bei Cyberangriffen eingebunden werden?

So früh wie möglich – spätestens sobald erste Ergebnisse der Forensik vorliegen, damit die datenschutzrechtliche Bewertung und Risikoanalyse beginnen kann.

Wie wird das Risiko für die betroffenen Personen bewertet?

Entscheidend sind zwei Faktoren: die mögliche Schwere des Schadens für die Betroffenen und die Wahrscheinlichkeit, dass er tatsächlich eintritt. Als erste Orientierung dient das Kurzpapier Nr. 18 der Datenschutzkonferenz (DSK) zum Thema „Risiko für die Rechte und Freiheiten natürlicher Personen“. Vom Ergebnis hängt ab, welche Melde- und Informationspflichten bestehen.



Warum sollte die Risikobewertung von Juristen vorgenommen werden?

Die Einstufung des Risikos ist eine rechtliche Bewertung mit weitreichenden Folgen. Sie entscheidet darüber, ob die Aufsichtsbehörde und die Betroffenen informiert werden müssen. Fehleinschätzungen können Bußgelder und Haftungsrisiken nach sich ziehen.

Muss auch eine nicht meldepflichtige Datenpanne dokumentiert werden?

Ja. Nach Art. 33 Abs. 5 DSGVO ist jede Verletzung intern zu dokumentieren, und zwar mit den Fakten, den Auswirkungen und den ergriffenen Abhilfemaßnahmen. Die Aufsichtsbehörde muss anhand dieser Dokumentation nachvollziehen können, ob die Entscheidung gegen eine Meldung vertretbar war.

Muss eine Datenpanne der Aufsichtsbehörde gemeldet werden?

Grundsätzlich ja. Nach Art. 33 DSGVO ist die Verletzung der zuständigen Datenschutzaufsichtsbehörde zu melden. Das gilt nur dann nicht, wenn sie voraussichtlich zu keinem Risiko für die Rechte und Freiheiten der betroffenen Personen führt.

Welche Frist gilt bei einer Datenpanne nach der DSGVO?

Die Meldung muss unverzüglich erfolgen, möglichst innerhalb von 72 Stunden. Die Frist beginnt, sobald das Unternehmen mit hinreichender Sicherheit von der Verletzung weiß. Sie läuft auch über Wochenenden und Feiertage. Fehlen noch Informationen, können Sie diese schrittweise nachreichen. Warten Sie mit der Meldung also nicht, bis die Untersuchung abgeschlossen ist. Wird die Frist überschritten, müssen Sie die Verzögerung begründen.

Bei welcher Datenschutzbehörde muss eine Datenpanne gemeldet werden?

Für Unternehmen in Bayern ist das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) zuständig. Es stellt ein Online-Meldeformular bereit. Die Meldung muss mindestens enthalten:

- die Art der Verletzung,
- die Kategorien und die ungefähre Zahl der betroffenen Personen und Datensätze,
- die Kontaktdaten des Datenschutzbeauftragten,
- die wahrscheinlichen Folgen und die Risikobewertung
- die ergriffenen oder geplanten Maßnahmen.

Wann müssen Betroffene über eine Datenpanne informiert werden?

Nach Art. 34 DSGVO dann, wenn die Verletzung voraussichtlich ein hohes Risiko für ihre Rechte und Freiheiten zur Folge hat. Die Betroffenen sind unverzüglich und in klarer, einfacher Sprache zu informieren über:

- die Art der Verletzung,
- die möglichen Folgen,
- die ergriffenen oder möglichen Maßnahmen,



- eine Anlaufstelle für weitere Informationen.

Was gilt, wenn der Angriff einen Dienstleister betrifft?

Ein Auftragsverarbeiter muss den Verantwortlichen unverzüglich informieren. Die Meldung an die Aufsichtsbehörde bleibt Pflicht des Verantwortlichen. Prüfen Sie daher die Meldefristen und Mitwirkungspflichten in Ihren Auftragsverarbeitungsverträgen. Ist Ihr Unternehmen selbst Dienstleister, müssen Sie Ihre Kunden unverzüglich informieren.

Welche Meldepflichten gelten nach NIS2 zusätzlich zur DSGVO?

Unternehmen, die unter das NIS2-Umsetzungsgesetz fallen, müssen zusätzlich an das BSI melden. Vorgesehen ist ein dreistufiges Verfahren: eine Frühwarnung innerhalb von 24 Stunden ab Verdacht, eine vollständige Meldung innerhalb von 72 Stunden und ein Abschlussbericht nach einem Monat. Diese Meldung kommt zur DSGVO-Meldung hinzu, hat eigene Inhalte und läuft über die Meldeplattform des BSI. Eine einmal abgegebene Meldung kann nicht zurückgezogen, sondern nur durch eine Folgemeldung korrigiert werden. Für Finanzunternehmen gilt außerdem DORA. Hinzu können vertragliche Informationspflichten gegenüber Kunden und Geschäftspartnern kommen.

Sollten Unternehmen nach einem Cyberangriff Strafanzeige erstatten?

Nicht jeder Hacking-Angriff ist strafbar. Ein frühes Einschalten der Strafverfolgungsbehörden kann aber bei der Aufklärung helfen und weitere Schäden verhindern. Eine Strafanzeige kann daher zu den geeigneten Maßnahmen gehören, mit denen Sie nachteilige Folgen begrenzen.

Welche Rolle spielt eine Cyberversicherung?

Eine Strafanzeige kann für den Versicherungsschutz relevant sein. Prüfen Sie deshalb frühzeitig die Vorgaben Ihres Versicherers, etwa Anzeige- und Mitwirkungsobliegenheiten, und berücksichtigen Sie diese bei allen weiteren Schritten.

Sollte man bei einem Ransomware-Angriff Lösegeld zahlen?

Behörden wie das BSI raten grundsätzlich davon ab. Eine Zahlung garantiert weder die Entschlüsselung noch die Löschung abgezogener Daten. Zudem können Sanktionsrecht, Versicherungsbedingungen und die Haftung der Geschäftsleitung berührt sein. Eine solche Entscheidung sollte nur nach rechtlicher Beratung getroffen werden.

Haftet ein Unternehmen automatisch, wenn es gehackt wurde?

Nein. Ein erfolgreicher Angriff beweist noch nicht, dass die Daten unzureichend geschützt waren. Das haben der EuGH und zuletzt das SG Nürnberg (Urteil vom 10.06.2026) bestätigt. Unternehmen müssen nicht jeden Angriff unter allen Umständen verhindern. Sie müssen aber geeignete technische und organisatorische Maßnahmen treffen, die zu den verarbeiteten Daten, zur Art der Verarbeitung und zu den Risiken für die Betroffenen passen.



Welche DSGVO-Bußgelder drohen bei einer nicht gemeldeten Datenpanne?

Verstöße gegen Art. 33 und 34 DSGVO können mit bis zu 10 Mio. Euro oder 2 % des weltweiten Jahresumsatzes geahndet werden. Die unterlassene Meldung ist dabei ein eigenständiger Verstoß, unabhängig davon, ob die Schutzmaßnahmen ausreichend waren.

Können Betroffene Schadensersatz verlangen?

Ja, wenn die Voraussetzungen nach Art. 82 DSGVO erfüllt sind. Es muss aber insbesondere ein Schaden und auch ein Verschulden des Unternehmens vorliegen. Nach größeren Vorfällen sollten Unternehmen zudem mit vermehrten Auskunftersuchen rechnen.

- die E-Mail-Adresse im Rahmen eines Verkaufs erhoben wurde
- der Widerspruchshinweis ordnungsgemäß erteilt wurde
- nur ähnliche eigene Produkte beworben werden
- kein Widerspruch oder Widerruf erfolgt ist.

Empfohlene Maßnahmen zur Umsetzung:

- Speicherung der Erhebungsquelle
- Dokumentation von Zeitpunkt und Inhalt der Hinweise
- Einrichtung technischer Prozesse zur sofortigen Verarbeitung von Widersprüchen
- Verwendung eines CRM- oder Datenschutzmanagementsystems (DSMS)

Verstöße können zu Bußgeldern nach Art. 83 DSGVO sowie abmahnfähigen Wettbewerbsverstößen führen.

