Bundesamt für Cybersicherheit

Die Meldung eines erheblichen Cybersicherheitsvorfalls durch Übermittlung dieses PDF-Formulars ist ausschließlich für jene Fälle vorgesehen, in denen die Verwendung des Meldeportals vorübergehend technisch nicht möglich ist. https://nim.services.usp.gv.at/at.gv.brz.nis2-public-p/nis2gvat/incidentsOverview/

# FRÜHWARNUNG

## zu erheblichem Cybersicherheitsvorfall gemäß § 34 Abs. 1 und Abs. 2 NISG 2026

### Name der Einrichtung und Kontaktinformationen

Name der meldenden Person:* _____

Name der Einrichtung:* _____

Geben Sie eine eindeutige Identifikationskennziffer der betroffenen Einrichtung an:* _____
(z.B. Kennziffer des Unternehmensregisters (KUR), Firmenbuchnummer, ZVR-Zahl udgl.)

Bezeichnung des Cybersicherheitsvorfalls:* _____
Geben Sie eine kurze, aussagekräftige Bezeichnung für den Cybersicherheitsvorfall an.

### Hauptansprechperson

Name:* _____

E-Mail-Adresse und/oder Telefonnummer:* _____

Funktion/Anmerkung: _____

### Weitere Ansprechpersonen, Funktionen und Erreichbarkeiten: (optional)

Hinweis: Die mit * gekennzeichneten Felder sind Pflichtfelder und müssen ausgefüllt werden.

## Betroffene Sektoren

Welche/n Sektor/en betrifft der Cybersicherheitsvorfall?*
(Mehrfachauswahl zulässig)

- ☐ Energie
- ☐ Verkehr
- ☐ Bankwesen
- ☐ Finanzmarktinfrastrukturen
- ☐ Gesundheitswesen
- ☐ Trinkwasser
- ☐ Abwasser
- ☐ Digitale Infrastruktur
- ☐ Verwaltung von IKT-Diensten (Business-to-Business)
- ☐ Öffentliche Verwaltung
- ☐ Weltraum
- ☐ Post- und Kurierdienste
- ☐ Abfallbewirtschaftung
- ☐ Produktion, Herstellung und Handel mit chemischen Stoffen
- ☐ Produktion, Verarbeitung und Vertrieb von Lebensmittel
- ☐ Verarbeitendes Gewerbe/Herstellung von Waren
- ☐ Anbieter digitaler Dienste
- ☐ Forschung

Betreiben Sie einen Vertrauensdiensteanbieter gemäß § 3 Z 17 oder Z 18 NISG 2026 und ist dieser vom Cybersicherheitsvorfall betroffen?*

- ☐ Ja
- ☐ Nein

Wenn ja, wäre unverzüglich, in jedem Fall aber **innerhalb von 24 Stunden nach Kenntnisahme** des Cybersicherheitsvorfalls eine **Meldung** gem. § 34 Abs. 2 Z 2 NISG 2026 zu übermitteln.

## Zeitpunkt und Dauer

Zeitangaben müssen in der zum betreffenden Zeitpunkt zutreffenden Mitteleuropäischen Zeit erfolgen.

Wann hat der Cybersicherheitsvorfall begonnen?*
(Datum und Uhrzeit) _____

Wann wurde der Cybersicherheitsvorfall erstmals erkannt bzw. zur Kenntnis genommen?*
(Datum und Uhrzeit) _____

## Ursache und Beschreibung

Ist der Cybersicherheitsvorfall auf rechtswidrige und schuldhafte Handlungen zurückzuführen?*

Diese Meldung ersetzt keine polizeiliche Anzeige.
Die Beantwortung dieser Frage mit „Ja" kann dazu führen, dass die zuständige Strafverfolgungsbehörde mit Ihnen in Verbindung tritt.

- ☐ Ja
- ☐ Nein
- ☐ Unbekannt

Beschreiben Sie den Cybersicherheitsvorfall:*

Bitte beschreiben Sie kurz die wesentlichen Aspekte des Cybersicherheitsvorfalls. Relevante Informationen können unter anderem mögliche Ursachen, die unmittelbaren Auswirkungen, die betroffenen Systeme sowie weitere für die Bewertung des Vorfalls wichtige Umstände umfassen. Nutzen Sie dieses Feld außerdem, um zusätzliche Informationen zum Cybersicherheitsvorfall anzugeben, die in den übrigen Datenfeldern nicht erfasst werden. Das Feld kann bei Bedarf bei jedem weiteren Bericht aktualisiert oder ergänzt werden.

## Auswirkungen des Vorfalls

Hat der Cybersicherheitsvorfall ausschließlich Auswirkungen in Österreich und sind grenzüberschreitende Auswirkungen derzeit auszuschließen?*

- ☐ Ja
- ☐ Nein

Welche Staaten sind betroffen?* (Mehrfachauswahl zulässig)

- ☐ Österreich
- ☐ Belgien
- ☐ Bulgarien
- ☐ Dänemark
- ☐ Deutschland
- ☐ Estland
- ☐ Finnland
- ☐ Frankreich
- ☐ Griechenland
- ☐ Irland
- ☐ Italien
- ☐ Kroatien
- ☐ Lettland
- ☐ Litauen
- ☐ Luxemburg
- ☐ Malta
- ☐ Niederlande
- ☐ Polen
- ☐ Portugal
- ☐ Rumänien
- ☐ Schweden
- ☐ Slowakei
- ☐ Slowenien
- ☐ Spanien
- ☐ Tschechische Republik
- ☐ Ungarn
- ☐ Zypern
- ☐ Island
- ☐ Liechtenstein
- ☐ Norwegen
- ☐ Schweiz

## Beschreiben Sie die Auswirkungen des Cybersicherheitsvorfalls:

Bitte beschreiben Sie die beobachteten und erwarteten Auswirkungen des Cybersicherheitsvorfalls, einschließlich einer Bewertung des Schweregrads und der Auswirkungen auf:

(a) die Erbringung der Dienstleistungen

(b) andere Unternehmen der Branche und/oder auf nationaler Ebene

(c) vor- oder nachgelagerte Lieferanten.

## Weitere Informationen

Unternehmensinterner Vorfall-Referenzcode: _____

Hier kann eine vorhandene interne Referenznummer angegeben werden, um einen Bezug zur eigenen Vorfallsbehandlung herzustellen.

Ist der Cybersicherheitsvorfall bereits öffentlich bekannt?*

- ☐ Ja
- ☐ Nein

Benötigen Sie eine Unterstützungsleistung durch das zuständige Computernotfallteam?

- ☐ Ja
- ☐ Nein

Wenn Ja, welche Unterstützungsleistungen des Computernotfallteams würden Sie benötigen?*

*Datenschutzhinweis*:
Die im Rahmen dieser Meldung erhobenen personenbezogenen Daten werden ausschließlich zum Zweck der Bearbeitung der Meldung und der Erfüllung der gesetzlichen Aufgaben nach dem Netz- und Informationssystemsicherheitsgesetz 2026 verarbeitet. Die Verarbeitung erfolgt auf Grundlage der einschlägigen gesetzlichen Bestimmungen.

☐ Ich bestätige hiermit die Richtigkeit der Angaben und stimme der Übermittlung und Verarbeitung zu.*

Wie geht es nun weiter?

- Übermitteln Sie das Formular dem zuständigen CSIRT.
- Das zuständige CSIRT wird sich mit Ihnen innerhalb der nächsten 24 Stunden nach Eingang Ihrer ersten Übermittlung zu diesem erheblichen Cybersicherheitsvorfall in Verbindung setzten und Sie im Sinne des § 34 Abs. 4 NISG 2026 unterstützen.
- Sollten Ihre Bekanntgaben rechtswidriges und schuldhaftes Handeln als Ursache nennen, kann die zuständige Strafverfolgungsbehörde mit Ihnen in Verbindung treten.
- Übermitteln Sie weitere Berichte, um den Status des erheblichen Cybersicherheitsvorfalls zu aktualisieren – dadurch unterstützen Sie die Tätigkeiten der CSIRTs und der Cybersicherheitsbehörde und tragen zum Lagebild bei. Beachten Sie dabei ggf. Fristen gemäß § 34 Abs. 2 NISG 2026.

| **Nationales CERT:** | **GovCERT:** | **Austrian HealthCERT:** |
|---|---|---|
| E-Mail: reports@cert.at | E-Mail: reports@govcert.gv.at | E-Mail: reports@a-healthcert.at |
| Tel.: +43 1 5056416 78 | Tel.: +43 1 5056416 930 | Tel: +43 720 704328 |
| Web: https://www.cert.at/ | Web: https://www.govcert.gv.at/ | Web: https://www.a-healthcert.at |

Die Zuständigkeit von CSIRTs richtet sich im Sinne des § 8 Abs. 3 und 4 NISG 2026 nach den Sektoren gemäß § 2 und den Anlage 1 und 2 zum NISG 2026. Derzeit bestehen folgende Zuständigkeiten:

- GovCERT — Sektor Öffentliche Verwaltung gemäß Z 10 Anlage 1 NISG 2026
- Austrian HealthCERT — Sektor Gesundheitswesen gemäß Z 5 Anlage 1 NISG 2026
- Nationales CERT — alle weiteren Sektoren gemäß Anlage 1 und 2 NISG 2026