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/

FORTSCHRITTSBERICHT

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

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) _____

Hält der Cybersicherheitsvorfall noch an?*

- ☐ Ja
- ☐ Nein

Wenn Nein, wann wurde der Cybersicherheitsvorfall erfolgreich behoben?* (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

Wählen Sie die zugrundeliegende(n) Ursache(n) des Cybersicherheitsvorfall aus:*
(Mehrfachauswahl zulässig)

☐ Böswilliges Handeln

Bitte wählen Sie die zutreffende/n böswillige/n Handlung/en aus:*
(Mehrfachauswahl zulässig)

- ☐ Vorsätzliche interne Handlungen
- ☐ Physische Beschädigung
- ☐ Schadsoftware
- ☐ Ransomware
- ☐ Informationsbeschaffung / Ausspähung
- ☐ Eindringversuche
- ☐ Eindringen / Kompromittierung
- ☐ Verfügbarkeitsangriffe (DoS, DDoS)
- ☐ Diebstahl / Sicherheit von Informationsinhalten
- ☐ Betrug
- ☐ Unbekannt
- ☐ Sonstiges

Liegen Ihnen Kompromittierungsindiktatoren (IOC – Indicator of Compromise) vor?*

- ☐ Ja
- ☐ Nein

Wenn Ja, Beschreibung IoC:*
(Falls Sie Zugang zu Informationen im Zusammenhang mit dem Cybersicherheitsvorfall haben, die zur Erkennung böswilliger Aktivitäten innerhalb eines Netzwerks oder Informationssystems beitragen können (Indicators of Compromise, kurz IoC), können Sie diese hier angeben. IoC-Informationen können die folgenden Datenkategorien umfassen: IP-Adressen, URL-Adressen, Domains, Datei-Hashes, Malware-Daten, Daten zur Netzwerkaktivität, Daten zu E-Mail-Nachrichte)

☐ Systemfehler/Fehlfunktion

Bitte wählen Sie die zutreffende/n Systemfehler/Fehlfunktionen aus:*
(Mehrfachauswahl zulässig)

- ☐ Hardwarekapazität und -leistung
- ☐ Hardwarewartung
- ☐ Hardwareverwaltung / Alterung
- ☐ Softwarekompatibilität / -konfiguration
- ☐ Softwareleistung
- ☐ Netzwerkkonfiguration
- ☐ Ausfall anderer genutzter Infrastruktur, z. B. Kühlung oder Stromversorgung
- ☐ Sonstiges

Liegen Ihnen Informationen zu Schwachstellen vor?*

- ☐ Ja
- ☐ Nein

Wenn Ja, beschreiben Sie diese.*

☐ Menschliches Versagen

Bitte wählen Sie die zutreffenden menschlichen Versagen aus:*
(Mehrfachauswahl zulässig)

- ☐ Fehler oder Unterlassung
- ☐ Unzureichende Ressourcen
- ☐ Fehlende Fähigkeiten & Fachkenntnisse
- ☐ Sonstiges

☐ Externes Ereignis

Bitte wählen Sie die zutreffende/n externen Ereignisse aus:*
(Mehrfachauswahl zulässig)

- ☐ Naturkatastrophen
- ☐ Sonstiges
- ☐ Höhere Gewalt

☐ Lieferkettenproblem

☐ Unbekannt

☐ Sonstiges

Erläutern Sie sonstige Angaben zu den Ursachen im Feld „Beschreiben Sie den Cybersicherheitsvorfall“.

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.

Erheblichkeit und Auswirkungen des Vorfalls

Welche Kriterien lassen den Cybersicherheitsvorfall als erheblich einstufen?*

(Mehrfachauswahl zulässig)

- ☐ Anzahl der betroffenen Nutzer
- ☐ Prozentsatz der betroffenen Nutzer
- ☐ Dauer des Ausfalls
- ☐ Geografische Ausbreitung
- ☐ Direkter finanzieller Verlust
- ☐ Immaterieller Schaden
- ☐ Materieller Schaden
- ☐ Reputationsschaden / Der Vorfall hat mediale Aufmerksamkeit erhalten
- ☐ Exfiltration von Geschäftsgeheimnissen oder anderen sensiblen Informationen
- ☐ Der Vorfall kann den Tod einer natürlichen Person verursachen
- ☐ Der Vorfall kann erhebliche Gesundheitsschäden bei natürlichen Personen verursachen
- ☐ Der Vorfall kann einen erfolgreichen, mutmaßlich böswilligen und unbefugten Zugriff auf Netzwerk- und Informationssysteme ermöglichen
- ☐ Das interne Krisenmanagement wurde aktiviert
- ☐ Betriebskontinuitätspläne wurde aktiviert
- ☐ Sonstiges

Erläutern Sie die sonstigen erheblichen Aspekte:*

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.

Handelte es sich um einen wiederkehrenden Cybersicherheitsvorfall?*

- ☐ Ja
- ☐ Nein
- ☐ Unbekannt

Wenn Ja, geben Sie nähere Informationen zum wiederkehrenden Cybersicherheitsvorfall an. Alternativ oder zusätzlich können Sie die Incident-ID angeben.
(Jede Meldung, die über das NIS2-Meldeportal abgegeben wurde, erhält eine Incident-ID. Sie finden diese in Ihrem Meldedashboard.)

Incident-ID: _____

Getroffene Maßnahmen

Wurden Abhilfe- bzw. Wiederherstellungsmaßnahmen getroffen oder sind solche geplant?*

- ☐ Ja
- ☐ Nein

Wenn Ja, beschreiben Sie die Abhilfe- bzw. Wiederherstellungsmaßnahmen näher:*

Wurden die Empfänger des betroffenen Dienstes über den Cybersicherheitsvorfall und über alle Maßnahmen sowie Abhilfemaßnahmen unterrichtet, die diese als Reaktion ergreifen können?*

- ☐ Ja
- ☐ Nein

Wurde eine Anzeige oder Meldung an weitere Behörden erstattet?*

☐ Ja
☐ Nein

Wenn ja, geben Sie an, wann und bei welcher Behörde die Anzeige oder Meldung erstattet wurde.*

(Bitte geben Sie hier auch vorhandene Geschäftszahlen der Anzeigen bzw. Meldungen an.)

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?*

Ist eine Behörde oder ein nationales CSIRT eines anderen EU-Mitgliedstaats beteiligt?

☐ Keine andere ausländische Behörde/Kein anderes ausländisches CSIRT ist beteiligt.
☐ Eine ausländische Behörde/ Ein ausländisches CSIRT wurde lediglich benachrichtigt.
☐ Eine aktive Unterstützung einer ausländischen Behörde/eines ausländischen CSIRTs wurde in Anspruch genommen.

Wenn ja, welche Behörde(n) war/en beteiligt und in welchem Staat befindet sich die jeweilige Behörde?

Name der Behörde/ des CSIRTs:*

Staat der Behörde/ des CSIRTs:* _____

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