

LEITFADEN · TOMORIS TOOLBOX

Ransomware-Angriff: Erste Hilfe für die ersten Stunden

Sofortmaßnahmen für die erste Stunde, den ersten Tag und die erste Woche, mit Meldepflichten nach NISG 2026 und DSGVO und einer Liste, was Sie lassen sollten

STAND

25.10.2026

UMFANG

PDF, 11 Seiten

ONLINE

tomoris.com/downloads/ransomware-erste-hilfe

AUF EINEN BLICK

1 h

Erste Stunde: isolieren statt ausschalten (BSI, CISA)

24 h

NIS2-Frühwarnung an das CSIRT (§ 34 NISG 2026)

72 h

Datenschutzmeldung (Art. 33 DSGVO)

0 €

Lösegeld: BK, BSI und CISA raten von Zahlung ab

FÜR WEN

- Geschäftsführung kleiner und mittlerer Unternehmen in Österreich, die im Ernstfall entscheiden muss
- IT-Leitung und Administration, die Systeme isoliert, Spuren sichert und den Wiederanlauf plant
- Notfall-, Datenschutz- und Informationssicherheitsverantwortliche, die Meldungen vorbereiten

WURUM ES GEHT

Wenn Ransomware zuschlägt, entscheiden die ersten Stunden darüber, ob sich der Schaden begrenzen lässt, Spuren erhalten bleiben und Meldefristen halten. Dieser Leitfaden ordnet die Sofortmaßnahmen nach erster Stunde, erstem Tag und erster Woche: Systeme isolieren, Beweise sichern, Zugangsdaten erneuern, über Lösegeld entscheiden, nach NISG 2026 und DSGVO melden, Anzeige erstatten und aus sauberen Sicherungen wieder anlaufen. Grundlage sind die Response Checklist von CISA, MS-ISAC, NSA und FBI, das BSI-Arbeitspapier zur Ersten Hilfe bei schweren IT-Sicherheitsvorfällen und die Hinweise des Bundeskriminalamts.

Dieser Leitfaden gibt einen Überblick über Sofortmaßnahmen und ersetzt weder einen Notfallplan noch Rechtsberatung oder forensische Unterstützung. Maßgeblich ist der Gesetzestext in der jeweils geltenden Fassung; ob eine Meldepflicht besteht, hängt von Ihrer Einrichtung und vom Vorfall ab. Die Kontaktliste ist an Ihr Unternehmen anzupassen.

INHALT

01	Die ersten Stunden auf einen Blick	3
02	Woran Sie einen Angriff erkennen	3
03	Isolieren, ohne Spuren zu vernichten	4
04	Beweise sichern	5
05	Zugänge sperren, Kennwörter erneuern	5
06	Lösegeld und Entschlüsselung	6
07	Melden: Pflichten, Anzeige, Versicherung	7
08	Wiederanlauf aus sauberen Sicherungen	8
09	Was Sie nicht tun sollten	9
10	Nachbereiten und Notfallkontakte festhalten	9
11	Quellen	10

01 —

Die ersten Stunden auf einen Blick

Was in der ersten Stunde, am ersten Tag, in der ersten Woche und danach zu tun ist.

Sofortmaßnahmen nach Zeit, zusammengestellt aus BSI, CISA, Bundeskriminalamt und NISG 2026



Erste Stunde

Eindämmen

Betroffene Systeme vom Netz trennen, nicht ausschalten. Keine Anmeldung mit Administratorkonten auf befallenen Geräten. Zeitpunkt der Kenntnisnahme festhalten, Notfallteam telefonisch alarmieren.



Erster Tag

Lagebild und Meldungen

Krisenstab einrichten, Spuren sichern, Schaden erfassen, Versicherung informieren, Anzeige erstatten. NIS2-pflichtige Einrichtungen senden die Frühwarnung spätestens 24 Stunden nach Kenntnisnahme.



Erste Woche

Bereinigen und anlaufen

Meldungen binnen 72 Stunden an CSIRT und Datenschutzbehörde. Einfallsweg suchen, Zugangsdaten von sauberen Geräten aus erneuern, Systeme neu aufsetzen und nach Priorität aus sauberen Sicherungen zurückholen.



Danach

Abschließen

NIS2-Abschlussbericht spätestens einen Monat nach der Meldung, Nachbesprechung, Maßnahmen. Bei vollständiger Kompromittierung nennt das BSI als Erfahrungswert 2 bis 4 Wochen Stillstand.

Die Zeitleiste ist eine Empfehlung von TOMORIS aus den genannten Quellen. CISA, MS-ISAC, NSA und FBI empfehlen, die ersten drei Schritte in Reihenfolge abzuarbeiten: isolieren, nur notfalls ausschalten, für den Wiederanlauf sichten (Teil 2, Schritte 1 bis 3). Gesetzlich vorgegeben sind nur die Meldefristen (Abschnitt 07).

02 —

Woran Sie einen Angriff erkennen

Warnsignale für alle Mitarbeitenden und Spuren, nach denen die Administration suchen sollte.

Eine Infektion zeigt laut BSI meist nach wenigen Tagen bis zwei Wochen ihre Wirkung; verschlüsselt wird häufig nachts oder am Wochenende (Kapitel 4.1). Mit einem Abfluss von Daten ist zu rechnen (Kurzfassung).

Warnsignale nach dem Bundeskriminalamt: Dateien lassen sich nicht öffnen oder tragen neue Endungen, eine Lösegeldforderung erscheint, Systeme werden ungewöhnlich langsam, Sicherheitssoftware ist deaktiviert, Konten sind gesperrt, Daten werden ungewöhnlich übertragen (Infoblatt, Präventionsseite).

Spuren für die Administration (CISA, Schritt 6; BSI, Anhang 6.5)

Neue oder hochgestufte Konten

Neu angelegte Konten im Active Directory, Konten mit erweiterten Rechten, auffällige Aktivität privilegierter Konten wie Domain Admins und ungewöhnliche Anmeldungen an VPN-Geräten (CISA).

Eingriffe in die Wiederherstellung

vssadmin.exe, wbadmin.exe, bcdedit.exe, fsutil.exe, wmic.exe

Ungewöhnliche Nutzung dieser Windows-Werkzeuge kann Sicherungen, Schattenkopien oder die Startkonfiguration beeinträchtigen; laut CISA eine verbreitete Technik, um die Wiederherstellung zu verhindern.

Ausgelesene Zugangsdaten, Datenabfluss

Mimikatz, NTDSutil.exe, Rclone

Hinweise auf ausgelesene AD- oder LSASS-Anmeldedaten und ungewöhnlich viel ausgehenden Datenverkehr, dazu unerwartete Fernwartungssoftware, neue Dienste und geplante Aufgaben (CISA).

Kontoänderungen in der Ereignisanzeige

4720, 4722, 4725, 4726, 4738, 4740, 4781

Event-IDs für Erstellung, Aktivierung, Deaktivierung, Löschung, Änderung, Sperrung und Umbenennung von Benutzerkonten (BSI, Anhang 6.5).

03 —

Isolieren, ohne Spuren zu vernichten

Die erste Stunde zum Abhaken: vom Netz trennen statt ausschalten, abgestimmt und über einen unabhängigen Kanal.

Grundregel: vom Netz trennen, nicht ausschalten. Die CISA schreibt zu Schritt 2 sinngemäß: Geräte nur ausschalten, wenn sie sich nicht vom Netz trennen lassen. Das verhindert, dass Infektionsartefakte und mögliche Beweise im flüchtigen Speicher erhalten bleiben, und soll nur geschehen, wenn sich weder das Netz vorübergehend abschalten noch der Host anders trennen lässt. Für die Forensik empfiehlt das BSI: erst ein Abbild des Arbeitsspeichers, dann hart vom Strom trennen statt herunterfahren (Kapitel 4.3).

- ☐ Betroffene Systeme bestimmen und sofort isolieren, kritische Systeme zuerst (CISA, Schritt 1).
- ☐ Bei vielen betroffenen Systemen das Netz am Switch trennen, möglichst alle gleichzeitig (CISA, Schritt 1; BSI, Kapitel 4.9).
- ☐ Sonst Netzkabel ziehen und WLAN trennen, Gerät nicht herunterfahren (BSI, Kurzfassung; Bundeskriminalamt).
- ☐ Abgestimmt isolieren und per Telefon koordinieren: Täter können beobachten, ob sie entdeckt wurden, und die Ransomware sonst vorher breit ausrollen (CISA, Schritt 1).
- ☐ Für betroffene Cloud-Ressourcen Snapshots der Volumes erstellen (CISA, Schritt 1).
- ☐ Keine Anmeldung mit Administratorkonten auf befallenen Systemen, solange sie im Netz hängen (BSI, Kapitel 4.2).
- ☐ Zeitpunkt der Kenntnisnahme notieren (Empfehlung von TOMORIS, Fristen nach § 34 Abs. 2 NISG 2026); Notfallteam, IT-Dienstleister und Cyber-Versicherung verständigen (Bundeskriminalamt; BSI, Kapitel 3.6).

04 —

Beweise sichern

Was Analyse, Versicherung und Anzeige brauchen und wie Sie es sichern, ohne es zu verändern.

Jede Aktion auf einem kompromittierten System kann Spuren verändern; arbeiten Sie möglichst nur an Kopien (BSI, Kapitel 4.3). Für eine Anzeige müssen Beweise gerichtsfest erhoben und Vorgänge dokumentiert werden; ohne eigene Forensik holen Sie früh externe Hilfe (Kapitel 3.7).

- ☐ Abbild von Arbeitsspeicher und Datenträgern einer Auswahl betroffener Geräte erstellen, auch virtueller und Cloud-Server (CISA, Schritt 9); am laufenden System nur noch das Speicherabbild (BSI, Kapitel 4.3).
- ☐ Datenträger als forensisches 1:1-Abbild sichern, das übliche Backup-Programme meist nicht können; bei virtuellen Maschinen das Verzeichnis der Virtualisierung sichern (BSI, Kapitel 4.3).
- ☐ Flüchtige Daten zuerst: Arbeitsspeicher, Windows-Sicherheitsprotokolle, Puffer der Firewall-Protokolle (CISA, Schritt 9).
- ☐ Protokolle von Proxy, E-Mail-Server, Firewall, Active Directory und Dateizugriffen sichern (BSI, Kapitel 4.4).
- ☐ Schadsoftware-Proben, Kompromittierungsindikatoren, Lösegeldforderung, verschlüsselte Beispieldateien und die Kommunikation mit den Tätern aufbewahren (CISA, Schritt 9 und Kasten bei Schritt 7).
- ☐ Uhrzeiten, Beobachtungen und Entscheidungen protokollieren, Screenshots sichern (Bundeskriminalamt, Infoblatt; BSI, Kapitel 3.7).

05 —

Zugänge sperren, Kennwörter erneuern

Täterzugänge schließen, Konten prüfen und Zugangsdaten von sauberen Geräten aus erneuern.

Bei Einbrüchen werden oft massenhaft Zugangsdaten abgegriffen (CISA, Schritt 13). Alle Zugangsdaten, die auf betroffenen Systemen gespeichert oder nach der Infektion dort eingegeben wurden, gelten als kompromittiert (BSI, Kurzfassung).

- Sofort externe Zugänge abschalten: VPN, Fernzugriffsserver, Single Sign-on und öffentlich erreichbare Cloud-Zugänge (CISA, Schritt 13).
- Systeme und Konten des ersten Einbruchs bestimmen, auch E-Mail-Konten, und alle Administratorkonten auf Legitimität prüfen (CISA, Schritt 12; BSI, Kapitel 4.2).
- Empfehlung von TOMORIS: Zugänge, die Täter von außen nutzen könnten, sofort und nur von sauberen Geräten aus ändern (Bundeskriminalamt: „Zugangsdaten unverzüglich ändern“; BSI, Kapitel 4.9).

- Nach der Bereinigung alle Administrator- und Dienstkennwörter sowie alle auf infizierten Systemen eingegebenen Kennwörter ändern, auch in Browsern, E-Mail-Programmen, RDP-Verbindungen und Fachverfahren (BSI, Kapitel 4.9; CISA, Schritt 17).
- Ist das Active Directory kompromittiert und nicht sofort neu aufzusetzen: das Kennwort des Kontos **KRBTGT** zweimal zurücksetzen, um gefälschte Kerberos-Tickets ungültig zu machen (BSI, Kapitel 4.9).
- Nicht nötige Fernzugänge etwa 2 bis 3 Wochen blockieren, Verbindungsversuche protokollieren und auswerten (BSI, Kapitel 4.9).

06 —

Lösegeld und Entschlüsselung

Was Behörden zur Zahlung sagen, was vor einer Entscheidung zu klären ist und wo es kostenlose Entschlüsselungswerkzeuge gibt.

Die Behörden raten einhellig ab. Das Bundeskriminalamt: „Zahlen Sie kein Lösegeld“; eine Zahlung garantiert weder die Entschlüsselung noch die Löschung gestohlener Daten, und Zahlende können erneut Ziel werden (Präventionsseite, Infoblatt). Das BSI: grundsätzlich nicht auf die Erpressung eingehen, sondern nach der Bereinigung aus intakten Sicherungen wiederherstellen (Kapitel 3.9). CISA, FBI, NSA und MS-ISAC empfehlen keine Zahlung, weil sie weder Entschlüsselung noch Schutz vor Veröffentlichung sichert (Kasten zu Beginn von Teil 2). Wird eine Zahlung dennoch erwogen, nennt das BSI diese Punkte (Kapitel 3.9):

- Die Cyber-Versicherung früh einbinden; sie macht oft Vorgaben für die Kostenübernahme.
- Mit Ermittlungsbehörden und Rechtsberatung abklären: Zahlungen finanzieren möglicherweise weitere Angriffe auf Dritte.
- Es gibt keine Garantie für einen passenden Schlüssel; vorab die Entschlüsselung einiger Beispieldateien verlangen.
- Auch nach der Entschlüsselung Systeme neu aufsetzen, weil Hintertüren bleiben können; nach einer Zahlung die Polizei informieren.

Kostenlose Entschlüsselung prüfen: Für manche Varianten gibt es Werkzeuge bei No More Ransom (nomoreransom.org), einer Initiative der niederländischen Polizei, von Europol und IT-Sicherheitsunternehmen; das Bundeskriminalamt verweist ausdrücklich darauf (Präventionsseite). Nicht jede Variante lässt sich entschlüsseln. Vorher die Schadsoftware entfernen, sonst wird erneut verschlüsselt (No More Ransom). Empfehlung von TOMORIS: an Kopien der verschlüsselten Daten arbeiten.

Droht die Veröffentlichung gestohlener Daten, lassen Sie die Leak-Seite der Täter beobachten, etwa durch einen Dienstleister. Werden Daten veröffentlicht, analysieren Sie sie und informieren die Betroffenen über Sachverhalt und Risiko (BSI, Kapitel 3.7 und 3.8). Fragen Sie auch die Strafverfolgungsbehörden nach verfügbaren Entschlüsselungswerkzeugen (CISA, Schritt 10).

07 —

Melden: Pflichten, Anzeige, Versicherung

NISG 2026 für pflichtige Einrichtungen, DSGVO bei personenbezogenen Daten, Anzeige bei der Polizei und vertragliche Pflichten.

Wesentliche und wichtige Einrichtungen melden jeden erheblichen Cybersicherheitsvorfall (§ 34 Abs. 1 NISG 2026). Erheblich ist er, wenn er schwerwiegende Betriebsstörungen oder finanzielle Verluste verursacht hat oder verursachen kann oder andere durch erhebliche Schäden beeinträchtigt hat oder beeinträchtigen kann (§ 35 Abs. 1). Jedenfalls erheblich ist er nach der NISV 2026 unter anderem, wenn es einen erfolgreichen, mutmaßlich böswilligen, unbefugten Zugriff gegeben hat, der wahrscheinlich schwerwiegende Betriebsstörungen verursacht, oder Notfallwiederherstellungspläne auslöst (§ 5 Abs. 1 Z 5 und 9; laut Erläuterungen für Einrichtungen außerhalb der DVO 2024/2690). Als Datenschutzverletzung zählen auch Vernichtung und Verlust personenbezogener Daten, nicht nur ihr Abfluss (Art. 4 Z 12 DSGVO).

Meldungen nach einem Ransomware-Angriff (Rechtsstand 25.10.2026)

MELDUNG	WER, WANN	FRIST	EMPFÄNGER, FUNDSTELLE
NIS2-Frühwarnung	wesentliche und wichtige Einrichtungen, erheblicher Vorfall	unverzüglich, spätestens 24 Stunden nach Kenntnisnahme	zuständiges CSIRT (§ 34 Abs. 1 und Abs. 2 Z 1 NISG 2026)
NIS2-Meldung	wie oben, mit erster Bewertung von Schweregrad und Auswirkungen	unverzüglich, spätestens 72 Stunden nach Kenntnisnahme	CSIRT (§ 34 Abs. 2 Z 2)
NIS2-Abschlussbericht	wie oben, mit Ursachen und Abhilfemaßnahmen	spätestens einen Monat nach der Meldung	CSIRT (§ 34 Abs. 2 Z 4)
Information der Kunden	wie oben, wenn der Vorfall Ihre Dienste beeinträchtigt	unverzüglich	Empfänger Ihrer Dienste (§ 34 Abs. 3)
Datenschutzmeldung	Verantwortliche, außer bei voraussichtlich keinem Risiko für Betroffene	unverzüglich, möglichst binnen 72 Stunden nach Bekanntwerden	Datenschutzbehörde (Art. 33 Abs. 1 DSGVO, § 18 Abs. 1 DSG)
Benachrichtigung Betroffener	Verantwortliche bei voraussichtlich hohem Risiko	unverzüglich	betroffene Personen (Art. 34 Abs. 1 DSGVO)
Strafanzeige	Geschädigte, empfohlen von Bundeskriminalamt und BSI	umgehend (Bundeskriminalamt)	jede Polizeidienststelle
Freiwillige Meldung	Einrichtungen außerhalb des NISG 2026	freiwillig	nationales CSIRT, auch anonym (§ 37 Abs. 2 und 3)

- Das CSIRT antwortet spätestens 24 Stunden nach Eingang der Frühwarnung und gibt bei vermutetem strafrechtlichem Hintergrund Orientierungshilfe für die Meldung an die Strafverfolgungsbehörden (§ 34 Abs. 4 NISG 2026).

- Die Meldestelle für Internetkriminalität im Bundeskriminalamt (against-cybercrime@bmi.gv.at) hilft bei Verdacht und Fragen; Anzeigen nimmt sie derzeit nicht entgegen, die erstatten Sie bei einer Polizeidienststelle (Bundeskriminalamt, Cybercrime). Bringen Sie das betroffene Gerät nach Möglichkeit mit (Präventionsseite).

Im Verfahren: Die EU-Kommission schlägt mit dem Digital-Omnibus vor, Datenschutzverletzungen nur noch bei voraussichtlich hohem Risiko und nach Möglichkeit binnen 96 Stunden zu melden (COM(2025) 837 vom 19.11.2025). Das Verfahren 2025/0360(COD) ist offen, im Europäischen Parlament steht laut Legislative Observatory die Ausschussentscheidung aus (Stand 25.10.2026). Bis dahin gelten 72 Stunden nach Art. 33 DSGVO.

08

Wiederanlauf aus sauberen Sicherungen

Priorisieren, sauber aufbauen, Sicherungen schützen und den Vorfall erst nach festgelegten Kriterien für beendet erklären.

1 Dienste einordnen und priorisieren

Ordnen Sie jede Dienstleistung ein: nicht betroffen, auslagerungsfähig, mit mobilem, nicht betroffenem Gerät eingeschränkt möglich, ohne Neuaufbau nicht möglich (BSI, Kapitel 3.4). Wiederhergestellt wird nach einer vorab erstellten Liste kritischer Systeme und der Systeme, von denen sie abhängen (CISA, Schritt 3).

2 Saubere Umgebung aufbauen

Beginnen Sie mit einem Kernnetz für kritische Geschäftsprozesse und erweitern Sie es systematisch (BSI, Kapitel 4.9). In ein eigenes VLAN für die Wiederherstellung kommen nur saubere Systeme (CISA, Schritt 19).

3 Neu aufsetzen statt bereinigen

Infizierte Systeme gelten als vollständig kompromittiert: neu aufsetzen, aktualisieren und härten, bevor sie ans Netz gehen. Ein kompromittiertes Active Directory ist langfristig neu aufzubauen (BSI, Kurzfassung und Kapitel 4.9).

4 Sicherungen prüfen und schützen

Finden Sie zuerst die Vorläufer-Schadsoftware, sonst geht die Kompromittierung nach dem Wiederherstellen weiter (CISA, Schritt 4). Arbeiten Sie mit Kopien der Sicherungen und legen Sie Bänder schreibgeschützt ein, damit übersehene infizierte Systeme sie nicht nachträglich infizieren (BSI, Kapitel 4.9).

5 Zurückspielen und abschließen

Spielen Sie Daten aus Offline-Sicherungen nach Priorität der kritischen Dienste zurück (CISA, Schritt 19). Für beendet erklärt den Vorfall die dafür benannte IT- oder IT-Sicherheitsleitung nach festgelegten Kriterien (Schritt 18).

Parallel einen Notbetrieb einrichten: Für den Notbetrieb wichtige Daten können noch auf nicht betroffenen Außenstellen oder auf Geräten von Mitarbeitenden im Urlaub liegen (BSI, Kurzfassung). Für Mitarbeitende, die ohne IT kaum arbeiten können, suchen Sie sinnvolle Aufgaben im Notbetrieb (Kapitel 3.2).

09

Was Sie nicht tun sollten

Typische Fehler der ersten Stunden, die den Schaden vergrößern, Spuren vernichten oder den Wiederanlauf gefährden.

- Nicht mit Administratorkonten an befallenen Systemen anmelden, solange sie im Netz sind (BSI, Kapitel 4.2).
- Nicht herunterfahren, solange sich das Gerät anders vom Netz trennen lässt (BSI, Kurzfassung; CISA, Schritt 2).
- Nicht über Kanäle koordinieren, die Täter mitlesen könnten, etwa das betroffene E-Mail-System (CISA, Schritt 1).
- Die Lösegeldforderung nicht löschen, sonst scheitert womöglich die Entschlüsselung (CISA, Kasten bei Schritt 7).
- Nicht nur das auffällige System bereinigen oder bloß den Virenschanner laufen lassen (BSI, Kapitel 4.1, Anhang 6.6).
- Sicherungen nicht an Systeme anschließen, die nicht nachweislich sauber sind (BSI, Kapitel 4.9).
- Nicht schweigen, niemanden beschuldigen, in E-Mails an Kunden keine Links verschicken (BSI, Kapitel 3.3, Anhang 6.6).
- Meldefristen nicht vergessen: Die 24 Stunden laufen ab Kenntniserlangung (§ 34 Abs. 2 Z 1 NISG 2026).

10

Nachbereiten und Notfallkontakte festhalten

Lehren aus dem Vorfall ziehen und die Kontakte eintragen, die Sie im Ernstfall sofort brauchen.

- Nachbesprechung: Was lief gut, was ist zu verbessern, welche langfristigen Maßnahmen folgen? Danach die IT von Externen prüfen lassen (BSI, Kapitel 3.10).
- Lehren dokumentieren und in Richtlinien, Pläne, Abläufe und Übungen übernehmen (CISA, Schritt 20).
- Den Notfallplan pflegen, regelmäßig üben und auch auf Papier und offline bereithalten (CISA, Teil 1).

Tragen Sie die Kontakte vorab ein, wie es die CISA mit ihrer Kontaktabelle empfiehlt (Abschnitt Contact Information, Tabelle 1), und halten Sie die Liste auch auf Papier bereit. Die Liste ist eine Vorlage von TOMORIS zum Anpassen.

Notfallkontakte zum Ausfüllen

STELLE	NAME, FUNKTION	TELEFON (RUND UM DIE UHR)	E-MAIL ODER MELDEWEG
Notfallleitung und Vertretung	_____	_____	_____
IT-Dienstleister, Incident Response	_____	_____	_____
Cyber-Versicherung, Polizzenummer	_____	_____	_____
Datenschutz und Rechtsberatung	_____	_____	_____
Kommunikation und Presse	_____	_____	_____
Zuständiges CSIRT (NIS2)	_____	_____	_____
Datenschutzbehörde	_____	_____	_____
Nächste Polizeidienststelle	_____	_____	_____
Meldestelle Bundeskriminalamt	Meldestelle für Internet-kriminalität	_____	against-cybercrime@bmi.gv.at

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

KOSTENLOS PRÜFEN

NIS2-Betroffenheitscheck

tomoris.com/tools/nis2-check

UMSETZUNG BESPRECHEN

Kontakt aufnehmen

tomoris.com/contact

contact@tomoris.com

11

Quellen

Alle Aussagen sind belegt. Gesetzestexte gelten in der jeweils geltenden Fassung.

- 1 CISA, MS-ISAC, NSA, FBI: #StopRansomware Guide, Version 3.0 (Oktober 2023)
Teil 1 (Vorbereitung), Teil 2 Response Checklist, Schritte 1 bis 20, Kästen zu Lösegeld und Ermittlerinformationen, Tabelle 1
www.cisa.gov/sites/default/files/2025-03/StopRansomware-Guide%20-%20Version%203.0.pdf
- 2 BSI: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall, Arbeitspapier Version 1.2 (07.10.2022)
Kurzfassung, Kapitel 3.2 bis 3.10, 4.1 bis 4.4, 4.9, 5, Anhänge 6.1, 6.5 und 6.6
[www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Th...](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Erste-Hilfe-bei-einem-schweren-IT-Sicherheitsvorfall-Arbeitspapier-Version-1.2.pdf?__blob=publicationFile)
- 3 Bundeskriminalamt: Ransomware – Informationen für Unternehmen in Österreich (Infoblatt, August 2026)
Beschreibung, Warnsignale, Sofortmaßnahmen, Hinweis zum Lösegeld
www.bundeskriminalamt.at/212/service/files/ransomware/324_2026_...
- 4 Bundeskriminalamt: Präventionsseite Ransomware
Warnsignale und Abschnitt „Was, wenn es mal passiert ist?“, Stand 18.08.2026
www.bundeskriminalamt.at/212/internet/ransomware.html

- 5 **Bundeskriminalamt: Cybercrime-Competence-Center C4 und Meldestelle against Cybercrime**
Meldestelle für Internetkriminalität und Anzeige, Stand 27.08.2026
www.bundeskriminalamt.at/306/start.html
- 7 **NISG 2026, BGBl. I Nr. 94/2025, geltende Fassung im RIS**
§§ 34, 35, 37 und 51, Fassung vom 25.10.2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...
- 9 **Bundesamt für Cybersicherheit: Erläuterungen zur NISV 2026 (PDF)**
Zu § 5: gilt für Sektoren außerhalb der DVO (EU) 2024/2690
www.bundesamt-cybersicherheit.gv.at/501/files/nisv-2026-erlaeut...
- 11 **Datenschutzgesetz (DSG), geltende Fassung im RIS**
§ 18 Abs. 1, Datenschutzbehörde als Aufsichtsbehörde
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...
- 6 **No More Ransom: Entschlüsselungs-Werkzeuge**
Hinweis vor dem Einsatz, Empfehlung zum Lösegeld; Träger laut Seite „Über das Projekt“
www.nomoreransom.org/de/decryption-tools.html
- 8 **NISV 2026, BGBl. II Nr. 290/2026, authentische Kundmachung im RIS**
§ 5 Abs. 1 Z 5 und 9, gelesen am 25.10.2026
www.ris.bka.gv.at/eli/bgbl/II/2026/290
- 10 **Verordnung (EU) 2016/679 (DSGVO)**
Art. 4 Z 12, Art. 33 und Art. 34
eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679
- 12 **EU-Kommission: Vorschlag für eine Digital-Omnibus-Verordnung, COM(2025) 837 vom 19.11.2025**
Neufassung von Art. 33 Abs. 1 DSGVO; Verfahren 2025/0360(COD), laut Legislative Observatory am 25.10.2026 offen
eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52025PC0837