

SPICKZETTEL · TOMORIS TOOLBOX

IT-Notfallkarte: Aushang für den Ernstfall zum Ausfüllen

Eine Seite zum Aufhängen mit Notfallnummern, Meldefragen und Verhaltensregeln, dazu Meldestellen in Österreich und die ersten Fragen für die IT

STAND

25.10.2026

UMFANG

PDF, 6 Seiten

ONLINE

tomoris.com/downloads/it-notfallkarte

AUF EINEN BLICK

1 Seite

zum Ausfüllen und Aufhängen

6

Fragen, die bei der Meldung beantwortet werden

3

Verhaltensregeln für alle Mitarbeitenden

12

Fragen für die IT nach einem Cyberangriff

FÜR WEN

- Alle Mitarbeitenden, für die die Karte an Arbeitsplätzen und in Fluren hängt
- IT-Leitung und Notfallverantwortliche, die die Karte ausfüllen und einführen
- Geschäftsführung kleiner und mittlerer Unternehmen ohne eigene IT-Abteilung
- IT-Dienstleister, die Notfallkarten für ihre Kunden vorbereiten

WURUM ES GEHT

Im IT-Notfall entscheiden die ersten Minuten: Wer bemerkt, dass etwas nicht stimmt, muss wissen, wen er anruft, was er sagt und was er besser nicht anfasst. Diese Notfallkarte folgt dem Aushang „Verhalten bei IT-Notfällen“ des deutschen Bundesamts für Sicherheit in der Informationstechnik und passt ihn an Österreich an. Seite 3 ist die Karte zum Ausfüllen und Aufhängen. Die weiteren Seiten erklären, wie Sie sie ausfüllen und einführen, welche Stellen in Österreich erreichbar sind und welche Fragen sich die IT nach einem Angriff stellen sollte.

Diese Notfallkarte ist eine Empfehlung von TOMORIS auf Grundlage der genannten Quellen und an Ihr Unternehmen anzupassen. Kontaktdaten Dritter entsprechen dem Stand 25.10.2026 laut den jeweiligen Stellen. Sie ersetzt kein Notfallhandbuch und keine Rechtsberatung zu Meldepflichten.

INHALT

01	So nutzen Sie diese Karte	2
02	Verhalten bei IT-Notfällen	3
03	So füllen Sie die Karte aus und führen sie ein	4
04	Externe Stellen in Österreich	4
05	Für die IT: zwölf Fragen nach einem Cyberangriff	5
06	Quellen	6

01 —

So nutzen Sie diese Karte

Die nächste Seite ist der Aushang; ausfüllen, ausdrucken und dort aufhängen, wo Mitarbeitende im Notfall nachsehen.

Das BSI versteht seine IT-Notfallkarte als Hinweisschild analog zum bekannten Aushang „Verhalten im Brandfall“. Sie stellt drei Botschaften in den Vordergrund: die Ansprechpartner für IT-Notfälle und ihre Erreichbarkeit kennen, entscheidende Informationen sofort weitergeben und Gegenmaßnahmen nur nach Absprache oder Anweisung setzen. Ob eine Fehlfunktion oder ein Angriff vorliegt, ist oft schwer zu erkennen; diese Entscheidung soll bei den zuständigen Personen liegen, nicht bei der Person, die den Notfall bemerkt.

Drucken Sie die nächste Seite einzeln aus, nachdem Sie die Felder ausgefüllt haben: Notfallnummern, Erreichbarkeit und Ihre Entscheidung zur Netztrennung. Alternativ erstellen Sie die Karte mit dem Werkzeug IT-Notfallkarte auf tomoris.com mit eigenen Ansprechpartnern und drucken sie in A4. Die Seiten danach sind für Notfallverantwortliche und IT bestimmt.

02 —

Verhalten bei IT-Notfällen

Ruhe bewahren und sofort melden. Lieber einmal zu viel anrufen als einmal zu wenig.

Wen Sie anrufen

WER	TELEFON	ERREICHBAR
IT-Notfallnummer	_____	_____
Vertretung	_____	_____
IT-Dienstleister	_____	_____
Geschäftsführung	_____	_____

Das sagen Sie am Telefon

Wer meldet?	Name, Abteilung, Rückrufnummer.
Welches Gerät?	Welcher Computer, welches Programm oder welcher Dienst ist betroffen?
Was getan?	Wie haben Sie zuletzt damit gearbeitet, etwa einen Anhang geöffnet?
Was gesehen?	Meldungen, gesperrte Dateien, ungewöhnliches Verhalten.
Wann?	Uhrzeit, zu der Sie es bemerkt haben.
Wo?	Gebäude, Raum, Arbeitsplatz.

- ☐ Weitere Arbeit am betroffenen Gerät einstellen
- ☐ Beobachtungen notieren, Bildschirm mit dem Diensthandy fotografieren
- ☐ Maßnahmen nur nach Anweisung der IT-Notfallnummer
- ☐ Bei Verdacht auf Schadsoftware: [Netzwerkkabel ziehen und WLAN ausschalten] oder [nur auf Anweisung]

Nicht selbst reparieren, nichts löschen, keine Zahlungen leisten. Bei Gefahr für Menschen: Polizei-Notruf 133 oder Euro-Notruf 112.

03

So füllen Sie die Karte aus und führen sie ein

Für Notfallverantwortliche und IT: Nummern eintragen, eine Entscheidung treffen, aufhängen, schulen, prüfen.

1

Notfallnummer festlegen

Tragen Sie eine Nummer ein, die im Ernstfall abgehoben wird, intern oder bei Ihrem IT-Dienstleister, und eine Vertretung. Das BSI sieht auf seiner Karte dafür ein Feld für die individuelle Rufnummer vor.

2

Netztrennung entscheiden

Legen Sie fest, ob Mitarbeitende bei Verdacht auf Schadsoftware selbst Kabel ziehen und WLAN ausschalten sollen. Das Bundeskriminalamt empfiehlt Unternehmen bei Ransomware, betroffene Systeme sofort vom Netzwerk zu trennen; das BSI rät Mitarbeitenden, Maßnahmen nur nach Anweisung zu setzen. Die Karte macht Ihre Entscheidung eindeutig.

3

Aufhängen

In Fluren, Arbeits- und Werkräumen und an IT-Arbeitsplätzen, überall dort, wo Mitarbeitende sie im Notfall finden sollen (BSI). Für Mitarbeitende anderer Sprachen bietet das BSI die Karte in zehn weiteren Sprachen an.

4

In Schulungen einführen

Das BSI empfiehlt, die Karte im Rahmen von Schulungen und Sensibilisierung vorzustellen und Mitarbeitende zu ermutigen, Auffälligkeiten zu melden.

5

Aktuell halten

Nummern bei jedem Personal- oder Dienstleisterwechsel prüfen, zusätzlich mindestens halbjährlich, und einmal im Jahr einen Testanruf außerhalb der Bürozeiten machen. Das ist eine Empfehlung von TOMORIS.

Das BSI erlaubt ausdrücklich, seine eigene Karte in der Organisation zu vervielfältigen, zu verbreiten und die Felder zu befüllen. Diese Karte von TOMORIS folgt ihrem Inhalt, ist aber eine eigene Fassung für Österreich.

04

Externe Stellen in Österreich

Für Notfallverantwortliche: wen Sie wann einbinden; Angaben laut den Stellen selbst, Stand 25.10.2026.

Meldestellen und Hilfe bei IT-Notfällen in Österreich

STELLE	WANN	KONTAKT LAUT STELLE
Polizei-Notruf, Euro-Notruf	Bei unmittelbar drohender Gefahr oder wenn die Polizei vor Ort gebraucht wird	133, 112
Polizeidienststelle	Anzeige einer Straftat, etwa nach einem Angriff oder einer Erpressung	jede Dienststelle; Servicenummer 059-133

Meldestelle für Internetkriminalität im Bundeskriminalamt	Verdacht auf Internetkriminalität, Hilfe und Informationen; eine Anzeige ist darüber derzeit nicht möglich	against-cybercrime@bmi.gv.at
CERT.at	Meldung von IT-Sicherheitsvorfällen; kein allgemeiner IT-Helpdesk	reports@cert.at, +43 1 5056416-78, Mo–Fr 8–18 Uhr an Werktagen
Cyber-Security-Hotline der Wirtschaftskammern	Telefonische Erstinformation und Notfallhilfe für Mitglieder	0800 888 133, täglich 0–24 Uhr
Datenschutzbehörde	Verletzung des Schutzes personenbezogener Daten: unverzüglich, möglichst binnen 72 Stunden (Art. 33 DSGVO)	laut Website der Datenschutzbehörde
Zuständiges CSIRT, nur für NIS2-Einrichtungen	Erheblicher Cybersicherheitsvorfall: Frühwarnung binnen 24 Stunden (§ 34 Abs. 2 Z 1 NISG 2026)	sektorspezifisches CSIRT, sonst nationales CSIRT

Ob eine Meldepflicht nach DSGVO oder NISG 2026 besteht, entscheidet die Geschäftsführung mit den Notfallverantwortlichen, nicht die meldende Person. Prüfen Sie Telefonnummern und Erreichbarkeiten beim Ausfüllen auf den Websites der Stellen.

05

Für die IT: zwölf Fragen nach einem Cyberangriff

Nach „TOP 12 Maßnahmen bei Cyber-Angriffen“ von BSI, Bundeskriminalamt (Deutschland) und Partnern, als Impuls, nicht als starre Reihenfolge.

- ☐ Erste Bewertung: Cyberangriff oder technischer Defekt?
- ☐ Maßnahmen laufend abgestimmt, dokumentiert und an alle Verantwortlichen kommuniziert?
- ☐ Protokolle, Log-Dateien, Notizen, Fotos von Bildschirmen und Datenträger forensisch gesichert?
- ☐ Besonders zeitkritische Geschäftsprozesse im Fokus?
- ☐ Betroffene Systeme und ihre Internetverbindungen getrennt, unautorisierte Zugriffe unterbunden?
- ☐ Backups gestoppt und vor weiteren Einwirkungen geschützt?
- ☐ Ausmaß der Ausbreitung festgestellt, alle angegriffenen Systeme identifiziert?
- ☐ Ausgenutzte Schwachstellen in Systemen und Prozessen behoben?
- ☐ Nach Abstimmung Polizei und Behörden benachrichtigt (Datenschutz, Meldepflichten)?

- ☐ Zugangsberechtigungen und Anmeldeverfahren betroffener Konten geprüft, etwa neue Passwörter und Zwei-Faktor-Anmeldung?
- ☐ Netzwerk nach dem Vorfall weiter überwacht?
- ☐ Betroffene Daten und Systeme wiederhergestellt oder neu aufgebaut?

Die Herausgeber betonen: Die Bewältigung eines Cyberangriffs ist stets individuell, die Maßnahmen sind an IT, Art des Angriffs und Ziele der Organisation anzupassen (TOP 12, Stand September 2019). Für die Planung vorab hilft ein IT-Notfallhandbuch.

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

KOSTENLOS PRÜFEN

IT-Notfallkarte

tomoris.com/tools/notfallkarte

NIS2-Meldefristen-Rechner

tomoris.com/tools/meldefristen-rechner

UMSETZUNG BESPRECHEN

Kontakt aufnehmen

tomoris.com/contact

contact@tomoris.com

06

Quellen

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

- 1 **BSI: IT-Notfallkarte „Verhalten bei IT-Notfällen“ (DIN A4)**
Meldefragen und Verhaltenshinweise
www.bsi.bund.de/SharedDocs/Downloads/Webs/ACS/DE/Notfallkarte/...
- 2 **BSI: IT-Notfallkarte, Anwendungshinweise und Nutzungsbedingungen**
Botschaften, Aushangorte, Schulung, Sprachen, Nutzungsbedingungen
www.bsi.bund.de/dok/13035678
- 3 **BSI und Partner: TOP 12 Maßnahmen bei Cyber-Angriffen, Stand September 2019**
zwölf Fragen, Vorbemerkung
www.bsi.bund.de/SharedDocs/Downloads/Webs/ACS/DE/Notfallkarte/T...
- 4 **Bundeskriminalamt: Ransomware, Informationen für Unternehmen in Österreich (v20260806)**
„Und wenn es mal passiert ist ...“
www.bundeskriminalamt.at/212/service/files/ransomware/324_2026...
- 5 **Bundeskriminalamt: Internetkriminalität, Meldestelle against Cybercrime**
letzte Aktualisierung 27.8.2026
www.bundeskriminalamt.at/306/start.html
- 6 **Polizei: Notrufe**
133, 112, Servicenummer 059-133
www.polizei.gv.at/alle/notrufe.aspx
- 7 **CERT.at: Kontakt**
Meldung von Sicherheitsvorfällen, Erreichbarkeit
www.cert.at/de/ueber-uns/kontakt
- 8 **WKO: Cyber-Security-Hotline der Wirtschaftskammern Österreichs**
Rufnummer, Erreichbarkeit, für Mitglieder
www.wko.at/it-sicherheit/cyber-security-hotline
- 9 **Verordnung (EU) 2016/679 (DSGVO), Art. 33**
Meldung an die Aufsichtsbehörde
eur-lex.europa.eu/eli/reg/2016/679/oj/deu
- 10 **NISG 2026, BGBl. I Nr. 94/2025, geltende Fassung im RIS**
§ 34 Abs. 1 und 2, Fassung vom 25.10.2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...