

GUIDE · TOMORIS TOOLBOX

Ransomware Attack: First Aid for the First Hours

Immediate measures for the first hour, the first day, and the first week, with reporting obligations under the NISG 2026 and the GDPR and a list of what you should avoid

UPDATED

Oct 25, 2026

LENGTH

PDF, 10 pages

ONLINE

tomoris.com/en/downloads/ransomware-erste-hilfe

AT A GLANCE

1 h

First hour: isolate instead of shutting down (BSI, CISA)

24 h

NIS2 early warning to the CSIRT (§ 34 NISG 2026)

72 h

Data breach notification (Art. 33 GDPR)

€0

Ransom: BKA, BSI and CISA advise against payment

WHO IT IS FOR

- Executive management of small and medium-sized companies in Austria who have to make decisions in an emergency
- IT management and administrators who isolate systems, secure traces, and plan the recovery
- Those responsible for emergencies, data protection, and information security who prepare the notifications

WHAT THIS COVERS

When ransomware strikes, the first hours determine whether the damage can be contained, traces are preserved, and reporting deadlines are met. This guide organizes the immediate measures by first hour, first day, and first week: isolate systems, secure evidence, renew credentials, decide on the ransom, report under the NISG 2026 (Austrian Network and Information Systems Security Act 2026) and the GDPR, file a criminal complaint, and restart from clean backups. It is based on the Response Checklist of CISA, MS-ISAC, NSA, and FBI, the BSI working paper on first aid for serious IT security incidents, and the guidance of the Austrian Federal Criminal Police Office (Bundeskriminalamt).

This guide provides an overview of immediate measures and replaces neither an emergency plan nor legal advice or forensic support. The statutory text in its current version is authoritative; whether a reporting obligation exists depends on your entity and the incident. The contact list must be adapted to your company.

CONTENTS

01	The first hours at a glance	3
02	How to recognize an attack	3
03	Isolate without destroying traces	4
04	Secure evidence	5
05	Block access, renew passwords	5
06	Ransom and decryption	6
07	Reporting: obligations, criminal complaint, insurance	6
08	Recovery from clean backups	8
09	What you should not do	8
10	Follow up and record emergency contacts	9
11	Sources	10

01 —

The first hours at a glance

What to do in the first hour, on the first day, in the first week, and afterward.

Immediate measures by time, compiled from BSI, CISA, the Federal Criminal Police Office, and the NISG 2026



First hour

Contain

Disconnect affected systems from the network, do not shut them down. Do not sign in with administrator accounts on infected devices. Record the time you became aware, alert the emergency team by phone.



First day

Situation picture and notifications

Set up a crisis team, secure traces, record the damage, inform the insurer, file a criminal complaint. Entities subject to NIS2 send the early warning no later than 24 hours after becoming aware.



First week

Clean up and restart

Notifications within 72 hours to the CSIRT and the Austrian Data Protection Authority (Datenschutzbehörde). Find the point of entry, renew credentials from clean devices, rebuild systems, and restore them from clean backups by priority.



Afterward

Close out

NIS2 final report no later than one month after the notification, debriefing, measures. In the case of full compromise, the BSI cites 2 to 4 weeks of downtime as a typical value.

The timeline is a TOMORIS recommendation based on the sources cited. CISA, MS-ISAC, NSA, and FBI recommend working through the first three steps in order: isolate, power down only if necessary, triage for recovery (Part 2, steps 1 to 3). Only the reporting deadlines are required by law (section 07).

02 —

How to recognize an attack

Warning signs for all employees and traces that administrators should look for.

According to the BSI, an infection usually takes effect after a few days to two weeks; encryption often happens at night or on weekends (chapter 4.1). You should expect data to have been exfiltrated (summary).

Warning signs according to the Federal Criminal Police Office: files cannot be opened or have new extensions, a ransom demand appears, systems become unusually slow, security software is disabled, accounts are locked, data is transferred unusually (information sheet, prevention page).

Traces for administrators (CISA, step 6; BSI, annex 6.5)

New or elevated accounts

Newly created accounts in Active Directory, accounts with elevated privileges, unusual activity of privileged accounts such as Domain Admins, and unusual sign-ins to VPN devices (CISA).

Interference with recovery

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

Unusual use of these Windows tools can impair backups, shadow copies, or the boot configuration; according to CISA, a common technique to prevent recovery.

Dumped credentials, data exfiltration

Mimikatz, NTDSutil.exe, Rclone

Indications of dumped AD or LSASS credentials and unusually high outbound data traffic, plus unexpected remote management software, new services, and scheduled tasks (CISA).

Account changes in Event Viewer

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

Event IDs for the creation, enabling, disabling, deletion, modification, lockout, and renaming of user accounts (BSI, annex 6.5).

03 —

Isolate without destroying traces

The first hour to check off: disconnect from the network instead of shutting down, coordinated and over an independent channel.

Basic rule: disconnect from the network, do not shut down. For step 2, CISA essentially states: power down devices only if they cannot be disconnected from the network. Doing so prevents infection artifacts and potential evidence in volatile memory from being preserved, and should only happen if the network can neither be taken offline temporarily nor the host be disconnected another way. For forensics, the BSI recommends: first take an image of the main memory, then cut the power hard instead of shutting down (chapter 4.3).

- ☐ Identify affected systems and isolate them immediately, critical systems first (CISA, step 1).
- ☐ If many systems are affected, disconnect the network at the switch, ideally all at the same time (CISA, step 1; BSI, chapter 4.9).
- ☐ Otherwise, unplug the network cable and disconnect Wi-Fi, do not shut down the device (BSI, summary; Federal Criminal Police Office).
- ☐ Isolate in a coordinated way and coordinate by phone: attackers may be watching whether they have been detected and may otherwise deploy the ransomware widely beforehand (CISA, step 1).
- ☐ Create snapshots of the volumes for affected cloud resources (CISA, step 1).
- ☐ Do not sign in with administrator accounts on infected systems while they are connected to the network (BSI, chapter 4.2).
- ☐ Note the time you became aware (TOMORIS recommendation, deadlines under § 34 para. 2 NISG 2026); notify the emergency team, IT service provider, and cyber insurer (Federal Criminal Police Office; BSI, chapter 3.6).

04 —

Secure evidence

What the analysis, the insurer, and the criminal complaint need and how you secure it without altering it.

Every action on a compromised system can alter traces; work only on copies wherever possible (BSI, chapter 4.3). For a criminal complaint, evidence must be collected in a court-admissible way and events documented; if you have no forensic capability of your own, get external help early (chapter 3.7).

- ☐ Create images of the main memory and storage drives of a selection of affected devices, including virtual and cloud servers (CISA, step 9); on a running system, take only the memory image (BSI, chapter 4.3).
- ☐ Secure storage drives as a forensic 1:1 image, which standard backup programs usually cannot do; for virtual machines, secure the virtualization directory (BSI, chapter 4.3).
- ☐ Volatile data first: main memory, Windows security logs, firewall log buffers (CISA, step 9).
- ☐ Secure logs from the proxy, email server, firewall, Active Directory, and file access (BSI, chapter 4.4).
- ☐ Keep malware samples, indicators of compromise, the ransom note, encrypted sample files, and the communication with the attackers (CISA, step 9 and box at step 7).
- ☐ Log times, observations, and decisions, save screenshots (Federal Criminal Police Office, information sheet; BSI, chapter 3.7).

05 —

Block access, renew passwords

Close attacker access, review accounts, and renew credentials from clean devices.

Intrusions often involve mass credential theft (CISA, step 13). All credentials stored on affected systems or entered there after the infection are considered compromised (BSI, summary).

- Immediately turn off external access: VPN, remote access servers, single sign-on, and publicly accessible cloud access (CISA, step 13).
- Identify the systems and accounts of the initial intrusion, including email accounts, and check all administrator accounts for legitimacy (CISA, step 12; BSI, chapter 4.2).
- TOMORIS recommendation: change access credentials that attackers could use from outside immediately and only from clean devices (Federal Criminal Police Office: "change credentials without delay"; BSI, chapter 4.9).
- After the cleanup, change all administrator and service passwords as well as all passwords entered on infected systems, including in browsers, email programs, RDP connections, and line-of-business applications (BSI, chapter 4.9; CISA, step 17).

- If Active Directory is compromised and cannot be rebuilt immediately: reset the password of the **KRBtgt** account twice to invalidate forged Kerberos tickets (BSI, chapter 4.9).
- Block unnecessary remote access for about 2 to 3 weeks, log and evaluate connection attempts (BSI, chapter 4.9).

06 —

Ransom and decryption

What the authorities say about paying, what to clarify before a decision, and where to find free decryption tools.

The authorities unanimously advise against it. The Federal Criminal Police Office: "Do not pay a ransom"; a payment guarantees neither decryption nor the deletion of stolen data, and those who pay may be targeted again (prevention page, information sheet). The BSI: as a rule, do not give in to the extortion, but restore from intact backups after the cleanup (chapter 3.9). CISA, FBI, NSA, and MS-ISAC do not recommend paying because it guarantees neither decryption nor protection against publication (box at the beginning of Part 2). If payment is nevertheless considered, the BSI names these points (chapter 3.9):

- Involve the cyber insurer early; it often sets conditions for covering costs.
- Clarify with law enforcement and legal counsel: payments may finance further attacks on third parties.
- There is no guarantee of a matching key; demand the decryption of a few sample files in advance.
- Rebuild systems even after decryption because backdoors may remain; after a payment, inform the police.

Check for free decryption: for some variants, tools are available from No More Ransom (nomoreransom.org), an initiative of the Dutch police, Europol, and IT security companies; the Federal Criminal Police Office explicitly refers to it (prevention page). Not every variant can be decrypted. Remove the malware first; otherwise, the data will be encrypted again (No More Ransom). TOMORIS recommendation: work on copies of the encrypted data.

If the publication of stolen data is threatened, have the attackers' leak site monitored, for example by a service provider. If data is published, analyze it and inform the affected persons about the facts and the risk (BSI, chapters 3.7 and 3.8). Also ask law enforcement about available decryption tools (CISA, step 10).

07 —

Reporting: obligations, criminal complaint, insurance

NISG 2026 for entities subject to it, GDPR for personal data, criminal complaint to the police, and contractual obligations.

Essential and important entities report every significant cybersecurity incident (§ 34 para. 1 NISG 2026). An incident is significant if it has caused or is capable of causing severe operational disruption or financial loss, or has affected or is capable of affecting others by causing considerable damage (§ 35 para. 1). Under the NISV 2026 (Austrian NIS Regulation 2026), it is significant in any case if, among other things, there has been successful, suspectedly malicious, unauthorized access that is likely to cause severe operational disruption, or if it triggers disaster recovery plans (§ 5 para. 1 nos. 5 and 9; according to the explanatory notes for entities

outside Implementing Regulation 2024/2690). A personal data breach also includes the destruction and loss of personal data, not only its exfiltration (Art. 4(12) GDPR).

Notifications after a ransomware attack (legal status as of October 25, 2026)

NOTIFICATION	WHO, WHEN	DEADLINE	RECIPIENT, CITATION
NIS2 early warning	Essential and important entities, significant incident	Without undue delay, no later than 24 hours after becoming aware	Competent CSIRT (§ 34 para. 1 and para. 2 no. 1 NISG 2026)
NIS2 incident notification	As above, with an initial assessment of severity and impact	Without undue delay, no later than 72 hours after becoming aware	CSIRT (§ 34 para. 2 no. 2)
NIS2 final report	As above, with causes and remedial measures	No later than one month after the notification	CSIRT (§ 34 para. 2 no. 4)
Information to customers	As above, if the incident affects your services	Without undue delay	Recipients of your services (§ 34 para. 3)
Data breach notification	Controllers, unless there is likely no risk to data subjects	Without undue delay, where feasible within 72 hours after becoming aware	Data Protection Authority (Art. 33(1) GDPR; § 18 para. 1 DSG, Austrian Data Protection Act)
Notification of data subjects	Controllers, if there is likely a high risk	Without undue delay	Data subjects (Art. 34(1) GDPR)
Criminal complaint	Victims, recommended by the Federal Criminal Police Office and the BSI	Immediately (Federal Criminal Police Office)	Any police station
Voluntary notification	Entities outside the NISG 2026	Voluntary	National CSIRT, also anonymously (§ 37 paras. 2 and 3)

- The CSIRT responds no later than 24 hours after receiving the early warning and, if a criminal background is suspected, provides guidance on reporting to law enforcement (§ 34 para. 4 NISG 2026).
- The Cybercrime Reporting Office of the Federal Criminal Police Office (against-cybercrime@bmi.gv.at) helps with suspicions and questions; it does not currently accept criminal complaints, which you file at a police station (Federal Criminal Police Office, Cybercrime). Bring the affected device with you if possible (prevention page).

In the legislative process: With the Digital Omnibus, the European Commission proposes that data breaches be reported only if there is likely a high risk, and where feasible within 96 hours (COM(2025) 837 of November 19, 2025). Procedure 2025/0360(COD) is open; according to the Legislative Observatory, the committee decision in the European Parliament is pending (as of October 25, 2026). Until then, the 72 hours under Art. 33 GDPR apply.

08 —

Recovery from clean backups

Prioritize, rebuild cleanly, protect backups, and declare the incident over only according to defined criteria.

1

Classify and prioritize services

Classify each service: not affected, can be outsourced, possible to a limited extent with a mobile, unaffected device, not possible without a rebuild (BSI, chapter 3.4). Restoration follows a previously created list of critical systems and the systems they depend on (CISA, step 3).

2

Build a clean environment

Start with a core network for critical business processes and expand it systematically (BSI, chapter 4.9). Only clean systems go into a dedicated VLAN for recovery (CISA, step 19).

3

Rebuild instead of cleaning

Infected systems are considered fully compromised: rebuild, update, and harden them before they go back online. A compromised Active Directory must be rebuilt in the long term (BSI, summary and chapter 4.9).

4

Check and protect backups

First find the precursor malware; otherwise, the compromise continues after restoration (CISA, step 4). Work with copies of the backups and insert tapes write-protected so that overlooked infected systems cannot infect them afterward (BSI, chapter 4.9).

5

Restore and close out

Restore data from offline backups according to the priority of critical services (CISA, step 19). The designated IT or IT security lead declares the incident over according to defined criteria (step 18).

Set up emergency operations in parallel: data important for emergency operations may still be stored at unaffected branch offices or on the devices of employees who are on vacation (BSI, summary). For employees who can hardly work without IT, find meaningful tasks during emergency operations (chapter 3.2).

09 —

What you should not do

Typical mistakes in the first hours that increase the damage, destroy traces, or jeopardize the recovery.

- Do not sign in with administrator accounts on infected systems while they are connected to the network (BSI, chapter 4.2).
- Do not shut down as long as the device can be disconnected from the network another way (BSI, summary; CISA, step 2).
- Do not coordinate over channels that attackers could be reading, such as the affected email system (CISA, step 1).

- Do not delete the ransom note; otherwise, decryption may fail (CISA, box at step 7).
- Do not clean only the conspicuous system or merely run the antivirus scanner (BSI, chapter 4.1, annex 6.6).
- Do not connect backups to systems that are not proven to be clean (BSI, chapter 4.9).
- Do not stay silent, do not blame anyone, do not send links in emails to customers (BSI, chapter 3.3, annex 6.6).
- Do not forget the reporting deadlines: the 24 hours run from the time you became aware (§ 34 para. 2 no. 1 NISG 2026).

10

Follow up and record emergency contacts

Learn lessons from the incident and enter the contacts you need immediately in an emergency.

- Debriefing: What went well, what needs to be improved, which long-term measures follow? Then have the IT reviewed by external parties (BSI, chapter 3.10).
- Document lessons learned and incorporate them into policies, plans, procedures, and exercises (CISA, step 20).
- Maintain the emergency plan, exercise it regularly, and keep it available on paper and offline as well (CISA, Part 1).

Enter the contacts in advance, as CISA recommends with its contact table (Contact Information section, Table 1), and keep the list available on paper as well. The list is a TOMORIS template for you to adapt.

Emergency contacts to fill in

CONTACT	NAME, ROLE	PHONE (24/7)	EMAIL OR REPORTING CHANNEL
Emergency lead and deputy	_____	_____	_____
IT service provider, incident response	_____	_____	_____
Cyber insurer, policy number	_____	_____	_____
Data protection and legal counsel	_____	_____	_____
Communications and press	_____	_____	_____
Competent CSIRT (NIS2)	_____	_____	_____
Data Protection Authority	_____	_____	_____
Nearest police station	_____	_____	_____
Federal Criminal Police Office reporting office	Cybercrime Reporting Office	_____	against-cybercrime@bmi.gv.at

NEXT STEP

Check It Yourself or Put It into Practice Together

CHECK FOR FREE

NIS2 applicability check (German)

tomoris.com/tools/nis2-check

DISCUSS IMPLEMENTATION

Get in Touch

tomoris.com/en/contact

contact@tomoris.com

11

Sources

All statements are supported by sources. Legislation applies in its current version.

- 1 **CISA, MS-ISAC, NSA, FBI: #StopRansomware Guide, Version 3.0 (October 2023)**
Part 1 (preparation), Part 2 Response Checklist, steps 1 to 20, boxes on ransom and investigator information, Table 1
www.cisa.gov/sites/default/files/2025-03/StopRansomware-Guide%20v3.0.pdf
- 2 **BSI: First aid for a serious IT security incident, working paper version 1.2 (October 7, 2022)**
Summary, chapters 3.2 to 3.10, 4.1 to 4.4, 4.9, 5, annexes 6.1, 6.5, and 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-fuer-einen-schweren-IT-Sicherheitsvorfall.pdf)
- 3 **Federal Criminal Police Office: Ransomware – information for companies in Austria (information sheet, August 2026)**
Description, warning signs, immediate measures, note on ransom
[www.bundeskriminalamt.at/212/service/files/ransomware/324_2026_...](https://www.bundeskriminalamt.at/212/service/files/ransomware/324_2026_01.pdf)
- 4 **Federal Criminal Police Office: Ransomware prevention page**
Warning signs and section "What if it has happened?", as of August 18, 2026
www.bundeskriminalamt.at/212/internet/ransomware.html
- 5 **Federal Criminal Police Office: Cybercrime Competence Center C4 and reporting office against cybercrime**
Cybercrime Reporting Office and criminal complaints, as of August 27, 2026
www.bundeskriminalamt.at/306/start.html
- 6 **No More Ransom: decryption tools**
Note before use, recommendation on ransom; sponsors according to the "About the project" page
www.nomoreransom.org/de/decryption-tools.html
- 7 **NISG 2026, BGBl. I No. 94/2025, current version in the RIS**
§§ 34, 35, 37, and 51, version as of October 25, 2026
[www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...](https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=105081000)
- 8 **NISV 2026, BGBl. II No. 290/2026, authentic promulgation in the RIS**
§ 5 para. 1 nos. 5 and 9, accessed October 25, 2026
www.ris.bka.gv.at/eli/bgbl/II/2026/290
- 9 **Federal Office for Cybersecurity: explanatory notes on the NISV 2026 (PDF)**
On § 5: applies to sectors outside Implementing Regulation (EU) 2024/2690
[www.bundesamt-cybersicherheit.gv.at/501/files/nisv-2026-erlaeut...](https://www.bundesamt-cybersicherheit.gv.at/501/files/nisv-2026-erlaeut.pdf)
- 10 **Regulation (EU) 2016/679 (GDPR)**
Art. 4(12), Art. 33, and Art. 34
eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679
- 11 **Datenschutzgesetz (DSG, Austrian Data Protection Act), current version in the RIS**
§ 18 para. 1, Data Protection Authority as supervisory authority
[www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...](https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=105081000)
- 12 **European Commission: proposal for a Digital Omnibus Regulation, COM(2025) 837 of November 19, 2025**
Revision of Art. 33(1) GDPR; procedure 2025/0360(COD), open on October 25, 2026, according to the Legislative Observatory
eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52025PC0837