computerforensic&more

The first hour.

Seven decisions that determine damage, recovery and investigation after a ransomware attack. Print it, put it in your crisis manual, pin it up next to the server room.

01 Isolate, don't shut down. ☐
Disconnect from the network, leave systems running. Power off only as a deliberate decision, with the time recorded.

02 Take backups offline. ☐
Disconnect backups immediately. Restore or rebuild nothing until the point of entry is known.

03 No contact with the attacker. ☐
Photograph the ransom note. Do not reply, do not open links. Whether to negotiate is a decision for management.

04 Communicate out of band. ☐
Not via company email or Teams. Treat privileged accounts as compromised. Disable them, don't delete them.

05 Start a timeline. ☐
Who noticed and did what, when, on which system. Every time with its time zone.

06 Insurer first. ☐
Notify your cyber insurer before engaging service providers. Many policies require it.

07 Check reporting obligations. ☐
Personal data affected? Notify the Austrian Data Protection Authority within 72 hours (Art. 33 GDPR). NIS entity? Early warning to the Federal Office for Cyber Security within 24 hours (NISG 2026).

INCIDENT RESPONSE · EMERGENCY HELP

Computerforensic & more GmbH

+43 (664) 144 83 63

YOUR NUMBERS · FILL IN BEFOREHAND

CRISIS MANAGEMENT	DEPUTY
CYBER INSURANCE, HOTLINE	POLICY NUMBER
IT SERVICE PROVIDER	DATA PROTECTION AND LEGAL