

BLUEPRINT

Incident Response

When an incident hits, speed and a well-run process make the difference.

Even the best protection can fail. Whether an incident ends as a minor nuisance or serious damage often depends on how quickly and how well the organisation responds. We help you prepare for incidents and handle them when they happen.

Before an incident

- an incident response plan with clearly assigned roles
- playbooks for the most common scenarios, such as ransomware or a compromised account
- crisis exercises

After an incident

- root-cause analysis and preservation of digital evidence
- recommendations to prevent a similar incident
- a final report

During an incident

- rapid assessment of scope and severity
- containment and stopping the attack
- removing the root cause and safely restoring operations
- support with communication and incident reporting – under NIS2, an early warning within 24 hours and an incident notification within 72 hours

What you get

- shorter downtime and less damage
- confidence that you know what to do when it counts
- compliance with legal incident-reporting obligations

AI

AI in practice AI speeds up log analysis and reconstruction of the incident timeline – decisions stay with people.

Who it's for any organisation that wants a plan ready for an incident rather than having to improvise.

Let's prepare for an incident before it happens.

info@anomalis.cz · +420 603 106 456 (24/7 for urgent cases) · www.anomalisit.cz

Anomalis IT s.r.o. · Korunní 2569/108, 101 00 Prague 10, Czech Republic · Company ID 09717404 · VAT ID CZ09717404