QUICK-REFERENCE SHEET · CRISIS MANAGEMENT

Cyberattack: the first 10 steps

The first hours of a cyberattack determine how much damage is done. Print this sheet and keep it at hand, outside your information system.

01 Isolate, do not switch off

Unplug the network cable and turn off Wi-Fi on affected machines. Do not shut them down: their memory holds traces useful to the investigation.

02 Raise the alarm immediately

Alert your IT team, CISO or provider, preferably by phone: email may be compromised.

03 Do not pay the ransom

Paying guarantees neither the recovery of your data nor that it will not be leaked. Do not contact the attackers.

04 Preserve the evidence

Delete nothing. Note times, displayed messages and abnormal behaviour. Keep the logs.

05 Activate the crisis team

Who decides, who acts, who communicates? Use a fallback communication channel, outside the information system.

06 Change passwords from a clean device

Administrator accounts and email first, from a device you know is not compromised.

07 Report

To the data protection authority within 72 hours if personal data is involved. If you are subject to NIS2, send an early warning to the authority within 24 hours. File a police report.

08 Get expert help

Call on a provider specialised in incident response. National cybersecurity agencies can point you to qualified professionals.

09 Notify your insurer

Your policy may set reporting deadlines and provide assistance. Check it now, not on the day of the attack.

10 Restart cleanly

Only bring systems back once the intrusion path is identified, on rebuilt systems and from clean backups.

Indicative sheet: adapt it to your organisation and add your emergency numbers (IT, management, provider, insurer).

GEN&SIS · Le Belvédère, 1-7 Cours Valmy, 92800 Puteaux

+33 6 76 72 78 61 · contact@genandsis.com · genandsis.com/en/