Infrastructure health check Rossi Meccanica Srl

On site: **14-15 October 2026** Delivered: **22 October 2026** Prepared by: **Karlken Alvarez** Version: **1.0**

01 Summary

3	4	3	0
high-priority risks	medium priority	low priority	restore tests ever run

Rossi Meccanica has 18 workstations, 2 servers (business app and files) and a NAS, all at the head office. The network works and the PCs are in good shape: day-to-day work is not at risk from performance problems.

The real risk is elsewhere: **today a NAS failure, a theft or ransomware would stop the office for days**. The only copy of the data sits in the same room as the servers and nobody has ever tried to restore it. On top of that, the business app is reachable from the Internet without a VPN, and 3 former employees' accounts are still active.

The three high priorities take about 3 days of work, plus around €8 a month for off-site storage.

02 What we checked

- Inventory of servers, NAS, PCs, printers and network services (192.168.10.0/24)
- Backups: what is copied, where, how often, and whether it can be restored
- Firewall, ports open to the Internet, VPN and remote access
- Accounts and passwords: active users, admins, former employees
- System updates, firmware and certificates

03 Risks found, by priority

#	AREA	WHAT WE FOUND	WHAT CAN HAPPEN	PRIORITY	ESTIMATE
R1	**Backups**	Only copy of the data on the office NAS; no restore test	Failure, theft or ransomware: data lost or days of downtime	HIGH	1.5 d
R2	**Access**	Remote desktop (RDP) to the business app open to the Internet, port 3389	Constant login attempts; a typical ransomware entry point	HIGH	0.5 d
R3	**Accounts**	3 former employees' accounts active; NAS with a shared "admin" user	Uncontrolled access, no trace of who does what	HIGH	2 h
R4	**Updates**	SRV-GEST (Windows Server 2016) unpatched for 9 months	Known vulnerabilities exploitable from the internal network	MEDIUM	0.5 d
R5	**Certificates**	Customer portal certificate expires in 12 days, renewed by hand	Portal unreachable or "not secure" for customers	MEDIUM	1 h
R6	**Network**	Guest Wi-Fi on the same network as the PCs and the server	An infected guest device sees the whole network	MEDIUM	0.5 d
R7	**Hardware**	NAS disk 2 with 14 reallocated sectors	The NAS has no margin left if another disk fails	MEDIUM	1 h + disk
R8	**Firewall**	Firewall firmware two years old	Missing security fixes	LOW	1 h
R9	**Documentation**	No network map or up-to-date list of services	Every job starts from scratch and takes longer	LOW	0.5 d
R10	**Printers**	Printer web panel with factory password	Unwanted configuration changes	LOW	30 min

Estimates are in working days and do not include hardware, licences or cloud services.

04 Recommended plan

THIS WEEK	Close port 3389 and let remote staff in through a VPN. Disable the 3 former employees' accounts, create named users on the NAS and change the admin password.
WITHIN 30 DAYS	Add an encrypted off-site copy (EU S3 storage, about €8/month per 1 TB, with versions that can't be deleted for 90 days). Run a documented restore test of the business app.
WITHIN 60 DAYS	Patch SRV-GEST in an evening window, turn on automatic certificate renewal, replace NAS disk 2 (about €90).
WHEN YOU CAN	Move guest Wi-Fi to its own VLAN, update the firewall firmware, change the printer passwords, keep the network map up to date.

05 Inventory at a glance

NAME	ROLE	ADDRESS	NOTES
SRV-GEST	Business app + database	192.168.10.10	Windows Server 2016
SRV-FILE	Shared folders	192.168.10.11	Windows Server 2019
NAS-01	Backup and archive	192.168.10.20	4 disks, RAID 5, 71% used
FW-01	Firewall / router	192.168.10.1	firmware 2024
PC	18 workstations	DHCP .100-.150	Windows 11, 2 to replace in 2027

06 Next steps

We go through it together in the one-hour call included in the health check. If you go ahead with one of the packages within 60 days, half of the health check is deducted.

Karlken Alvarez

DevOps & infrastructure consultant · Milan