CICADA | RESOURCES

LESSON 02 OF 03 · 7 MIN · WORKING KNOWLEDGE

Remote access without the front door open

Exposed remote desktop is a favourite target. Here's how to give people access without leaving a login on the internet.

The exposed desktop problem

Remote Desktop Protocol (RDP) lets someone control a Windows machine. It's useful, and it should never be reachable directly from the internet. Automated scanners find open RDP constantly and try leaked passwords. A single account without MFA can hand over a machine.

The same applies to web admin panels, VNC, SSH and old VPN appliances.

Replace direct exposure

- Turn off port forwarding for RDP and admin panels.
- Use a VPN or zero-trust access service with MFA.
- If RDP is unavoidable, put it behind a gateway with MFA and restrict source addresses.
- Use the provider's secure access rather than exposing a console.
- Patch the remote-access software itself.

Who, when, and what happened

Give access to named people, not a shared account. Review the list quarterly and remove leavers the same day. Restrict hours or require re-approval where the tool allows it. Review logs for failed logins, unexpected countries and odd hours.

If nobody reads the logs, the control is decorative.

ONE EXPOSED PORT IS ENOUGH

You don't need a sophisticated breach. An open RDP port and a reused password can be all it takes. Ask your provider to confirm, in writing, that nothing is exposed.

Key takeaways

- ✓ Never expose RDP directly to the internet.
- ✓ Use VPN or zero-trust access with MFA.
- ✓ Restrict access to named users and review regularly.
- ✓ Read the logs or the control isn't working.