From Remote Desktop Protocol to Domain Administrator

Now, for tomorrow

How one weak control can expose the entire network

It can start with one remote login. Remote Desktop Protocol (RDP) lets employees and IT teams access a computer or server from another location. It is useful, but if it is poorly protected, it can become an open door into the organisation.
An attacker may need only a weak password, a stolen login or an account without multi-factor authentication. Once inside the first computer, the attacker can look for saved passwords, confidential information and links to other systems.

THE ATTACK PATH: Weak remote access >Compromised computer > Stolen administrator credentials >Control of the network

This movement through the network is often called lateral movement. In simple terms, the attacker uses one compromised system to reach the next, collecting more access at each stage. If administrator passwords are reused, user permissions are too broad or important systems are not separated, the route to the most powerful accounts becomes much shorter.

Now, for tomorrow

Why Domain Administrator access matters

A Domain Administrator account is effectively a digital master key. It can provide control over most computers, user accounts and systems within the organisation. Once an attacker reaches this level, containing the incident becomes significantly more difficult because they may be able to change security settings and hide their activity.

- View or steal sensitive business information.
- Create new accounts and maintain hidden access.
- Disable security tools, lock employees out or spread ransomware.
- Interrupt critical services and business operations.

For the business, the consequences can include operational downtime, financial loss, regulatory exposure and damage to customer trust. What began as one poorly protected remote connection can quickly become an organisation-wide crisis.

Now, for tomorrow

The lesson: protect the entire path

RDP itself is not necessarily the problem. The danger comes from weak controls around it: poor passwords, missing multi-factor authentication, excessive user access, reused administrator accounts, limited monitoring and systems that are not properly separated. Remote access should be protected through multi-factor authentication, secure gateways or Virtual Private Networks (VPNs), limited user permissions and active monitoring. Administrator accounts should be separate from everyday user accounts and used only when necessary. Regular vulnerability assessments and penetration tests can also show how several small weaknesses might connect to create a much larger risk.

Now, for tomorrow

The question is not simply, “Is our remote access secure?” It is, “If one remote account were compromised today, how far could an attacker go?”

Now, for tomorrow