RDP (Remote Desktop Protocol) Security

With many staff still working from home companies will be evaluating business processes to enable their staff to get the most out of their working set up. With this comes further cybersecurity challenges. We want to highlight the following advice for companies using RDP (Remote Desktop Protocol) to improve RDP security.

Remote desktop is an application that allows the user to control the desktop — and, indeed, the entire contents — of one computer from a second machine.

Allowing another computer to control another machine, makes security extremely important. Anyone running the software, even if the connection is direct wired, should make sure that the connection is secure and password protected to reduce the possibility that an unauthorised user could access the remote computer.

Tips for RDP deployment –

- Deny access to Remote Desktop Protocols (RDP) directly from the internet
    - Block all access to RDP.
    - Utilise a VPN with multifactor authentication, if internet based access to RDP is required.

- Limit internal network machine to machine RDP
    - Apply appropriate internal network segmentation.
    - Deny standard workstations to arbitrarily connect to servers or other workstations over RDP (or any other unnecessary protocol).
    - Limit RDP to servers, ideally critical devices should not have RDP enabled.

- Audit your network for systems using RDP for remote communication. Disable the service if unneeded or install available patches. Users may need to work with their technology vendors to confirm that patches will not affect system processes.
- Enable strong passwords and account lockout policies to defend against brute-force attacks.
- Apply two-factor authentication, where possible.
- Apply system and software updates regularly.
- Maintain a good back-up strategy.

- Enable logging and ensure logging mechanisms capture RDP logins. Keep logs for a minimum of 90 days and review them regularly to detect intrusion attempts.
- When creating cloud-based virtual machines, adhere to the cloud provider's best practices for remote access.
- Ensure third parties that require RDP access are required to follow internal policies on remote access.

As part of the cross-government Cyber Aware campaign, GCHQ's National Cyber Security Centre (NCSC) has launched the free of use Cyber Action Plan tool for individuals and small business to receive advice on improving their cyber security in an increasingly digital world.

This alert was sent out for your information by Police Scotland
Cybercrime Prevention Unit - PPCWCyberHarmPrevention@Scotland.pnn.police.uk
All information was correct at time of distribution.