Remote Access Best Practices

Encryption
Access must use encrypted protocols. For example, SSH or similar must be used instead of telnet or FTP, and RDC or similar must be used instead of VNC.

Reverse Authentication
Where possible, access should use protocols which require the remote server to authenticate to the connecting user as well as vice versa. This two-way authentication helps protect against man in the middle attacks. For example, SSH tracks host keys, while RDC contains no server authentication mechanism.

Cryptographic Authentication
Access must use cryptographic authentication rather than password authentication wherever possible. For example, SSH private keys and USB smart cards must be used instead of passwords.

Password Protection
Users must protect their cryptographic authentication credentials with a password known only to themselves. This password must be new and not used for any other purpose, especially for their UNet account.

Limited exposure
Users must limit the exposure of their cryptographic authentication credentials.

Software certificates, etc.
If the user does not employ an external device, he should keep one copy of the credential on each of his personal computers and a single backup copy on non-network accessible storage such as a USB flash drive. The user must maintain the security of all personal computers storing a copy of his credentials.

Server-to-Server Access
Where possible, users' credentials should be used for access instead of direct access between servers.

Allowable situations
Direct access between servers must only be used in the following situations:

Automation
Direct access between servers is appropriate for automating non-interactive processes that involve more than one server.

Moot access
Direct access between servers is appropriate in cases where the design of the servers is such that compromising the trusted server entails access to the trusting server.

Limitation of access
The extent of the access between servers must be limited as much as possible. This limitation includes commands or functions that can be performed as well as the user context in which the commands run. For example, if the only essential function is to transfer files, then no further access should be allowed.

External devices
If the user employs an external device such as a USB smart card, he should keep one copy of the credential on that device and a single backup copy on non-network accessible storage such as a USB flash drive.

Related articles
- Remote Access Best Practices
- Set Up RDC for Windows XP
- Set Up RDC for Windows 10
- Set Up RDC for Windows 7
- Secure Shell (SSH)