16.5. Remote Access

Objective

16.5.1. Remote access to systems is secure, controlled and authorised.

Context

Scope

16.5.2. This section covers information relating to the methods used by personnel to access an agency system from a remote location.

Remote access

16.5.3. Remote access is defined as user access to agency systems originating outside an agency network. It does not include web–based access to DMZ resources. Further information on working off–site can be found in Chapter 21 – Distributed working. The requirements for using multi–factor authentication are described in the Identification and Authentication section of this chapter.

Remote privileged access

16.5.4. Remote access by a privileged user to an agency system via a less trusted security domain (for example, the Internet) may present additional risks. Controls in this section are designed to prevent escalation of user privileges from a compromised remote access account.

16.5.5. Remote privileged access does not include privileged access across disparate physical sites that are within the same security domain or privileged access across remote sites that are connected via trusted infrastructure. Privileged access of this nature faces different threats to those discussed above. Ensuring robust processes and procedures are in place within an organisation to monitor and detect the threat of a malicious insider are the most important measure for this scenario.

Encryption

16.5.6. Cryptography is used to provide confidentiality and preserve integrity of data transmitted over networks where it may be intercepted or examined and is outside the control of the sender and recipient.

16.5.7. With the increases in speed and computing power and the cost reductions of modern computing, older cryptographic algorithms are increasingly vulnerable. It is vital that recommendations and controls in the NZISM are followed.

16.5.8. The use of approved cryptographic algorithms to encrypt authentication, session establishment and data for all remote access connections is considered good practice (See Chapter 17 - Cryptography and Chapter 21 - Distributed Working).

References

16.5.9. Further references can be found at:

Title	Publisher	Source
Multi-Site Connectivity	NSA	Capability Packages (nsa.gov)
NIST Special Publication 800-114: User's Guide to Telework and Bring Your Own Device (BYOD) Security	NIST	SP 800-46 Rev. 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security | CSRC

Rationale & Controls

Authentication

16.5.10.R.01. **Rationale**

Authenticating remote system users and devices ensures that only authorised system users and devices are allowed to connect to agency systems.

16.5.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1973]

Agencies MUST authenticate each remote connection and user prior to permitting access to an agency system.

16.5.10.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1974]

Agencies SHOULD authenticate both the remote system user and device during the authentication process.

Remote privileged access

16.5.11.R.01. **Rationale**

A compromise of remote access to a system can be limited by preventing the use of remote privileged access from an untrusted domain.

16.5.11.C.01. **Control System Classifications(s): Top Secret, Secret, Confidential; Compliance: Must Not** [CID:1977]

Agencies MUST NOT allow the use of remote privileged access from an untrusted domain, including logging in as an unprivileged system user and then escalating privileges.

16.5.11.C.02. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:1978]

Agencies SHOULD NOT allow the use of remote privileged access from an untrusted domain, including logging in as an unprivileged system user and then escalating privileges.

Virtual Private Networks (VPNs)

16.5.12.R.01. **Rationale**

Virtual Private Networks (VPN's) use a tunnelling protocol to create a secure connection over an intermediate (public) network such as the internet. A VPN uses techniques such as encryption, authentication, authorisation and access control to achieve a secure connection. See Chapter 17 for details on cryptographic selection and implementation.

16.5.12.R.02. **Rationale**

A VPN can connect remote or mobile workers or remote locations to a private (agency) network.

16.5.12.R.03. **Rationale**

Using Zero Trust principles alongside the use of VPNs provides additional security to agency systems. For example, if a compromised device connects through a VPN to an organisation enforcing Zero Trust principles, potential damage to the organisation will be minimised through limiting the access of the potential compromise.

16.5.12.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1982]

Agencies SHOULD establish VPN connections for all remote access connections.

16.5.12.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7555]

Agencies SHOULD use Zero Trust principles alongside the use of VPN connections to enhance the security posture of the organisation. This should include removing the ability for a standard user to disable the VPN connection.