National Cyber Security Centre
a part of GCHQ

Guidance (/)

10 Steps: Network Security

Created: 01 Oct 2015
Updated: 08 Aug 2016
Part of: 10 Steps to Cyber Security (/guidance/10-steps-cyber-security)
This section from within the NCSC's '10 Steps To Cyber Security' concerns Network Security.

Summary

The connections from your networks to the Internet, and other partner networks, expose your systems and technologies to attack. By creating and implementing some simple policies and appropriate architectural and technical responses, you can reduce the chances of these attacks succeeding (or causing harm to your organisation).

Your organisation's networks almost certainly span many sites, and the use of mobile / remote working, and cloud services, makes defining a fixed network boundary difficult. Rather than focusing purely on physical connections, think also about where your data is stored and processed, and where an attacker would have the opportunity to interfere with it.

What is the risk?

Networks need to be protected against both internal and external threats. Organisations that fail to protect their networks appropriately could be subject to a number of risks, including:

- **Exploitation of systems:** Ineffective network design may allow an attacker to compromise systems that perform critical functions, affecting the organisations ability to deliver essential services or resulting in severe loss of customer or user confidence.
- **Compromise of information**: A poor network architecture may allow an attacker to compromise sensitive information in a number of ways. They may be able to access systems hosting sensitive information directly or perhaps allow an attacker to intercept poorly protected information whilst in transit (such as between your end user devices and a cloud service).
- **Import and export of malware:** Failure to put in place appropriate security controls could lead to the import of malware and the potential to compromise business systems. Conversely users could deliberately or accidentally release malware or other malicious content externally with associated reputational damage.
- **Denial of service:** Internet-facing networks may be vulnerable to Denial Of Service (DOS) attacks, where access to services and resources are denied to legitimate users or customers.
- **Damage or defacement of corporate resources:** Attackers that have successfully compromised the network may be able to further damage internal and externally facing systems and information (such as defacing your organisation's websites, or posting onto your social media accounts), harming the organisation’s reputation and customer confidence.

How can the risk be managed?

Produce, implement and maintain network security designs and policies that align with the organisation’s broader risk management approach. It may be helpful to follow recognised network design principles (eg ISO 27033) to help define an appropriate network architecture including both the network perimeter, any internal networks, and links with other organisations such as service providers or partners.

Manage the network perimeter: Manage access to ports, protocols and applications by filtering and inspecting all traffic at the network perimeter to ensure that only traffic which is required to support the business is being exchanged. Control and manage all inbound and outbound network connections and deploy technical controls to scan for malicious content:

- **Use firewalls:** Use firewalls to create a buffer zone between the Internet (and other untrusted networks) and the networks used by the business. The firewall rule set should deny traffic by default and a whitelist should be applied that only allows authorised protocols, ports and applications to exchange data across the boundary. This will reduce

the exposure of systems to network based attacks. Ensure you have effective processes for managing changes to avoid workarounds.

- **Prevent malicious content**: Deploy malware checking solutions and reputation-based scanning services to examine both inbound and outbound data at the perimeter in addition to protection deployed internally. The antivirus and malware solutions used at the perimeter should ideally be different to those used to protect internal networks and systems in order to provide some additional defence in depth.

Protect the internal network: Ensure that there is no direct routing between internal and external networks (especially the Internet), which limits the exposure of internal systems to network attack from the Internet. Monitor network traffic to detect and react to attempted or actual network intrusions.

- **Segregate networks as sets**: Identify, group and isolate critical business systems and apply appropriate network security controls to them.
- **Secure wireless access:** All wireless access points should be appropriately secured, only allowing known devices to connect to corporate Wi-Fi services. Security scanning tools may be useful to detect and locate unauthorised or spoof wireless access points.
- **Enable secure administration:** Administrator access to any network component should properly authenticated and authorised. Make sure default administrative passwords for network equipment are changed.
- **Configure the exception handling processes:** Ensure that error messages returned to internal or external systems or users do not include sensitive information that may be useful to attackers.
- **Monitor the network:** Network intrusion detection and prevention tools should be deployed on the network and configured by qualified staff. The capabilities should monitor all traffic for unusual incoming and outgoing activity that could be indicative of an attack. Alerts generated by the system should be promptly managed by appropriately trained staff.
- **Assurance processes**: Conduct regular penetration tests of the network architecture and undertake simulated cyber attack exercises to ensure that security controls have been well implemented and are effective.

Learn more

- Our guidance on Security Operations and Monitoring(/guidance/security-operations-centre-soc-buyers-guide) can help you design and implement approaches to maintaining security of a deployed network.
- Read our Cloud Security Guidance(/guidance/cloud-security-collection).

Further reading

Security operations centre (SOC) buyers guide(/guidance/security-operations-centre-soc-buyers-guide)
Cloud Security Collection(/guidance/cloud-security-collection)

Topics

Network security(/topics/network-security)
Cyber attacks(/topics/cyber-attacks)

Was this guidance helpful?

We need your feedback to improve this content.

Yes No