Part 7: Establish Basic Perimeter Defences

Introduction

Cyber criminals can take advantage of devices and networks that connect to the Internet. Organizations can establish safer networks and protect sensitive, important data by implementing simple perimeter defences.

Firewalls

To defend against online threats, organizations should use a dedicated firewall as it can prevent people and devices from connecting to harmful websites and among other malicious activities. Firewalls act as gated borders in a network, controlling the flow of (authorized and unauthorized) web activity. They set choke points to direct web traffic, and keep track of the connections and traffic in audit logs. They are a security measure used to restrict access to a private network or its devices. A firewall's main job is to regulate and enforce network access. They manage access by establishing a policy rule, which broadly defines access based on traffic source and destination.

The security infrastructure of an organization's firewall must be safeguarded from exploitation. To secure it, it is crucial to disable insecure protocols, plan regular backups, enable auditing of system changes, add rules to conceal the firewall from network scans, restrict management access to certain hosts, and use role-based access control for firewall administrators.

Wi-Fi networks should be secure and offer robust user authentication, like the use of the WPA2 wireless security protocol. Organizations should also implement security safeguards to safeguard their email services, like Domain-based Message Authentication, Reporting, and Conformance (DMARC). DMARC is an email authentication, policy, and reporting system that can recognize and stop email address forgeries.

A policy statement related to setting up basic perimeter defences:

- Deploy a dedicated firewall at the corporate network/Internet interface.
- Demand Multifactor Authentication and/or adopt a strong password policy.
- Rename or modify default accounts and passwords.
- Build a DNS firewall for outgoing DNS requests to the Internet.
- Employ secure VPN connectivity with two-factor authentication for remote access to the business network.
- Utilize secure Wi-Fi for internal networks.
- Make specific access roles and accounts for DevSecOps teams.
- Avoid linking publicly available Wi-Fi networks to the corporate network.
- Configure DMARC for email security.
- Delegate and limit access to fit the user's requirement for access.

References

Canadian Centre for Cyber Security. “Establish Basic Perimeter Defences.” *Canadian Centre for Cyber Security*, Government of Canada / Gouvernement Du Canada, 6 Sept. 2019, https://www.cyber.gc.ca/en/guidance/establish-basic-perimeter-defences