

Security Controls

Firewalls and
Intrusion Detection
Secure e-mails

By

Prof. Muhammad Iqbal Bhat

Department of Higher Education
Government Degree College Beerwah

Topics:

1

What are Security Controls

2

Types of Security Controls

3

Firewalls

4

Intrusion Detection

5

Secure e-mails

Prof. M. Iqbal Bhat (JKHED)

Security Controls

Security controls are measures taken to protect data and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

Security controls can be used to implement security policies and procedures, to enforce compliance with legal and regulatory requirements, and to reduce the risk of security incidents and breaches.

There are three types of security controls:

Administrative

Technical

Physical.

Administrative Security Controls:

Administrative security controls are policies, procedures, and guidelines that are implemented to manage security risks and ensure compliance with legal and regulatory requirements.

They focus on ensuring that employees and contractors follow established security procedures and best practices.

Examples of administrative security controls include:

- Security policies and procedures that define roles and responsibilities, access control, incident response, and risk management procedures.
- Security awareness training for employees to promote good security practices and reduce the risk of human error.
- Background checks and security clearances for employees and contractors to ensure that they are trustworthy and reliable.
- Security audits and reviews to evaluate the effectiveness of security controls and identify potential vulnerabilities.

Technical Security Controls

Technical security controls are technologies that are used to prevent unauthorized access, detect and respond to security incidents, and protect data and information systems.

They focus on the use of technology to mitigate security risks and enforce security policies.

Examples of technical security controls include:

- Firewalls that monitor and filter network traffic to prevent unauthorized access and block malicious traffic.
- Intrusion detection and prevention systems (IDS/IPS) that detect and respond to security incidents.
- Antivirus software that detects and removes malware from computers and devices.
- Encryption that protects data in transit and at rest from unauthorized access.
- Access control mechanisms that require authentication, authorization, and auditing of user access to systems and data.

Technical Security Controls

Physical security controls are measures that are taken to protect physical access to data and information systems.

They focus on protecting physical infrastructure, devices, and systems from unauthorized access and damage.

Examples of physical security controls include:

- Access controls that limit access to data centers, server rooms, and other areas that house sensitive information.
- Surveillance cameras and alarms that detect and deter unauthorized access or intrusions.
- Environmental controls such as fire suppression systems and temperature and humidity monitoring to prevent damage to hardware and data.
- Physical security assessments to evaluate the effectiveness of physical security controls and identify potential vulnerabilities.

Conclusion:

Security controls are critical components of an effective security program that help to protect sensitive information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

Organizations should use a combination of administrative, technical, and physical security controls to manage risk and ensure compliance with legal and regulatory requirements.

Effective security controls require ongoing monitoring and assessment to ensure that they remain effective in the face of changing threats and vulnerabilities.

Firewalls

A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Firewalls are designed to prevent unauthorized access to a network or computer system, and to block malicious traffic and attacks.

Firewalls can be implemented in hardware or software, and can be configured to enforce specific security policies and rules.

Types of Firewalls

1

Packet-filtering firewalls that examine individual packets of data and filter traffic based on IP addresses, port numbers, and protocols.

2

Stateful inspection firewalls that maintain a record of the state of connections and use this information to filter traffic.

3

Application-level gateways (or proxies) that filter traffic at the application layer and provide additional security by analyzing application-specific data.

4

Next-generation firewalls (NGFW) that incorporate advanced features such as intrusion prevention, malware detection, and application identification and control.

Firewall Functionality

1

Firewalls operate by enforcing security policies and rules that are configured by network administrators.

2

They examine incoming and outgoing traffic and filter packets based on predetermined criteria.

3

Firewalls can be configured to block traffic based on IP addresses, port numbers, protocols, or specific application data.

4

They can also log and report on network activity, and alert administrators to potential security threats and incidents.

Firewall Placement:

- Firewalls can be placed in various locations within a network, depending on the specific security needs and objectives of the organization.
- Examples of firewall placement include:
 - I. Border firewalls that are placed between an internal network and the Internet to protect against external threats.
 - II. Internal firewalls that are placed within a network to protect specific segments or systems from internal threats.
 - III. Host-based firewalls that are installed on individual devices to provide additional security for specific applications or services.

Firewall Limitations

Firewalls have limitations and cannot protect against all types of security threats.

They are only effective against attacks that can be filtered based on the predetermined security policies and rules.

Firewalls cannot protect against attacks that exploit vulnerabilities in applications or systems.

They cannot protect against threats that originate from within a network, such as insider threats or attacks that use stolen credentials.

Intrusion Detection Systems

An intrusion detection system (IDS) is a security technology that monitors network or computer systems for signs of unauthorized access or malicious activity.

IDS works by analyzing network traffic and system events to identify suspicious or anomalous behavior that may indicate a security breach or attack.

IDS can be used to detect a wide range of security threats, including network scanning, denial-of-service (DoS) attacks, malware, and insider threats.

Types of Intrusion Detection Systems

1

Network-based intrusion detection systems (NIDS) that analyze network traffic to detect security threats and anomalies.

2

Host-based intrusion detection systems (HIDS) that analyze system events and logs on individual devices to detect security threats and anomalies.

Network-based Intrusion Detection Systems

NIDS are designed to monitor network traffic and identify suspicious behavior that may indicate a security threat or attack.

NIDS work by analyzing network packets and comparing them to known signatures of malicious activity or anomalous behavior.

Examples of NIDS include Snort, Suricata, and Bro.

Host-based Intrusion Detection Systems


HIDS are designed to monitor system events and logs on individual devices to detect security threats and anomalies.

HIDS work by analyzing system activity and comparing it to known signatures of malicious activity or anomalous behavior.

Examples of HIDS include OSSEC, Tripwire, and McAfee Endpoint Security.

Functionality of Intrusion Detection System

IDS operate by analyzing network traffic or system events to identify suspicious activity or security threats.



IDS can be configured to alert administrators or automated response systems when potential threats or attacks are detected.



IDS can also log and report on network activity and security events, providing valuable insights for threat analysis and incident response.

Limitations of Intrusion Detection Systems

IDS have limitations and cannot protect against all types of security threats.

IDS rely on known signatures of malicious activity or anomalous behavior, which can be circumvented by attackers using sophisticated evasion techniques.

IDS cannot protect against vulnerabilities in applications or systems, and cannot prevent insider threats or attacks that use stolen credentials.

Secure Email:



Secure email refers to the use of encryption and other security technologies to protect email communications from interception or unauthorized access.



Secure email is important for protecting sensitive or confidential information, and for complying with legal and regulatory requirements for data protection.

Prof. Milind Bhat (UKIEM)

Secure Email Technologies

- There are several technologies used to secure email communications:
 - **Secure Sockets Layer (SSL) and Transport Layer Security (TLS):** These are cryptographic protocols that encrypt email messages and protect them from interception or tampering in transit.
 - **Pretty Good Privacy (PGP) and GNU Privacy Guard (GPG):** These are open-source encryption programs that use public-key cryptography to encrypt and decrypt email messages.
 - **S/MIME:** Secure/Multipurpose Internet Mail Extensions is a protocol that uses digital certificates to encrypt and digitally sign email messages.

Secure Email Examples



Gmail offers SSL/TLS encryption for emails in transit, and S/MIME encryption for messages sent between Gmail accounts.



ProtonMail is a secure email provider that uses end-to-end encryption to protect all email messages and attachments.



Microsoft Outlook offers S/MIME encryption for email messages, as well as a feature called "Message Encryption" that allows users to send encrypted messages to recipients who may not use S/MIME.



Mozilla Thunderbird is an email client that supports PGP encryption through the use of add-ons.

Best Practices for Secure Email:

Use	Use a strong password for email accounts and enable two-factor authentication.
Encrypt	Encrypt sensitive or confidential email messages using encryption technologies such as S/MIME or PGP.
Avoid	Avoid sending sensitive or confidential information through email whenever possible, and instead use secure file-sharing services or encrypted messaging apps.
Keep	Keep email clients and software up-to-date to ensure the latest security patches and updates are installed.
Be	Be cautious of phishing emails and other email scams, and avoid opening attachments or clicking links from unknown or suspicious senders.



Prof. M. Iqbal Bhat (JKHED)

Questions?

