E-Commerce

Saviya Varghese
BCA

What should a firewall contain?

- The firewall should be able to support a “deny all services except those specifically permitted" design policy, even if that is not the policy used.
- The firewall should support your security policy, not impose one. (impose-force on someone)
- The firewall should be flexible; it should be able to accommodate new services and needs if the security policy of the organization changes.
- The firewall should contain advanced authentication measures or should contain the provision for installing advanced authentication measures.
- The firewall should employ filtering techniques to permit or deny services to specified host systems as needed.

- The IP filtering language should be flexible, user-friendly to program, and should filter on as many attributes as possible, including source and destination IP address, protocol type, source and destination TCP/UDP port, and **inbound** and **outbound** interface.

Inbound-connections coming in to a specific device from a remote location
Outbound-connections going out to a specific device from a device.

- The firewall should use proxy services for services such as FTP and TELNET, so that advanced authentication measures can be employed and centralized at the firewall.

- If services such as NNTP(N/W NEWS TRANSFER PROTOCOL), X, http, or gopher(distributing, searching,retreiving documents in internet protocol n/w) are required, the firewall should contain the corresponding proxy services.

- The firewall should contain the ability to centralize SMTP access, to reduce direct SMTP connections between site and remote systems. This results in centralized handling of site e-mail.

- The firewall should accomodate public access to the site, such that public information servers can be protected by the firewall but can be segregated (separated) from site systems that do not require the public access.

- The firewall should contain the ability to concentrate and filter dial-in access. (dial in connection to company is not used by non employees to gain access to company information s/m resources)

•The firewall should contain mechanisms for logging traffic and suspicious activity, and should contain mechanisms for log reduction so that logs are readable and understandable.

•If the firewall requires an operating system such as UNIX, a secured version of the operating system should be part of the firewall, with other security tools as necessary to ensure firewall host integrity. The operating system should have all patches installed.

The firewall should be developed in a manner that its strength and correctness is verifiable. It should be simple in design so that it can be understood and maintained.

•The firewall and any corresponding operating system should be updated with patches and other bug fixes in a timely manner

BENEFITS OF FIREWALL

A Firewall can protect both individual computers and corporate networks from security threats.

1. Monitors Traffic
2. Blocks Trojans
3. Stops Hackers
4. Stops Keyloggers

Monitors Traffic

- A firewall monitors all of the traffic entering your computer network.
- A two-way firewall does double duty and monitors the traffic exiting your network as well.(Two -way firewall:provides incoming &outgoing n/w request detection)
- Information is sent over networks in packets. Those packets are what the firewall investigates to determine if there's something they contain that's potentially hazardous to your network's security.

2.Blocks Trojans

- A firewall helps block Trojan horses.

- These types of intruders(attacker) enter onto your computer files, and then when you send out a file, they go along for the ride to do more damage at the destination.

- Trojans are especially dangerous because they silently transmit information about us to a Web server.

- A firewall blocks them from the outset, before they have a chance to infect your computer.(outset-start /beginning of something)

3. Stops Hackers

- Firewall blocks hackers out of our network.

- Without firewall security, a hacker could get a hold of our computer and make it a part of large group of computers used to conduct illicit(illegal) activity, such as spreading viruses.

➢While hackers represent an extreme group, individuals who you may not suspect, such as neighbors, can also take advantage of an open Internet connection you may have. A firewall prevents such intrusions.

4.Stops Keyloggers

➢ Firewall security will reduce the risk of keyloggers monitoring our system.

➢ A keylogger is spyware software that cybercriminals try to put on your computer so they can target your keystrokes.

➢After they can identify what we are typing in and where, they can use that information to do the same thing. This knowledge can help them log in to our private online accounts.

Keylogging-without the user consent or knowledge that everything they type is being saved for later by whoever is spying on them

Limitations of firewall

❑ The firewall cannot protect against attacks that bypass the firewall.

❑ The firewall may not protect fully against internal threats

❑ An improperly secured wireless LAN may be accessed from outside the organization

❑ A portable storage device may be used and infected outside the corporate n/w ,and then attached and used internally.

Defining an enterprise-wide security framework

Enterprise risk mgmt refers to a common framework applied by business mgmt to identify potential events that may affect the enterprise, manage the risks and opportunities and provide reasonable assurance that company's objectives will be achieved.

Through this framework, organisation can achieve the following:-

1. Organisation can ensure prompt solution of internally identified risk to compliance with laws and regulations and to maintain the provision of quality products,protect safety and ensure appropriate relationship with customers.(prompt solution-quick solution)

Defining an enterprise-wide security framework continued…….

2.It provides support strategies to ensure effective use of resources and enable a better approach to auditing and identification resolution of compliance issues and promote reporting and monitoring across compliance functions.

3.Enable improved decision making,planning and prioritization through a structured understanding of opportunities and threats.

4.Support value creation by enabling mgmt to deal with future events that create uncertainty ,create a significant risk or opportunity and to respond in a prompt(done without delay), efficient and effective manner.

Value creation:The performance of actions that increase the worth of goods,services, or even a business.

5.Support growth drivers of creating value through innovation, extending global reach with local focus,executing with excellence and leading with purpose.

Components of Enterprise Risk mgmt Framework

1.Event identification and risk assessment

2.Risk response

3.Control activities

4.Information and communication

5.Monitoring

1.Event identification and risk assessment

- Functional leaders identify internal and external events.
- Risk mgmt function personnel (people employed in an organization)help identify &assess these risks through their experience, formal assesments and analysis of business intelligence &trends.

2.Risk response

- It is determined on the basis of overall risk exposure.
- It includes avoiding, accepting,reducing and sharing risk.

3.Control activities

- Ctrl activities are established to ensure that risk responses are carried out effectively &constantly throughout the organization.

- It involves i)formalizing risk response in company policies
  ii)ensuring clear accountability
  iii)utilizing self assessment
  iv)monitoring tools & designing controls into systems
  v)critical business processes

4.Information and communication

Information and communication channels are essential to make the organization aware of risks that fall into their area of responsibility and expected behaviour and actions to mitigate negative outcomes.

5.Monitoring

- Mgmt reviews risk mgmt activities which include testing , auditing &assessments.

- It is essential to ensure that risks are effectively identified &assessed and that appropriate responses,ctrls and preventive actions are taken.

Thank you