UNIT III

CYBER SECURITY FOR BUSINESS APPLICATIONS AND NETWORKS

Business Application Management

- Business application management and security is a complex field. Applications encompass purpose-built applications developed in-house or by contractors, applications supplied by application and operating system vendors, and open source application software. Applications may operate ona variety of platforms, including workstations, PCs, mobile devices, and web based. They may also need to access and generate a wide variety of data files and databases.

CORPORATE BUSINESS APPLICATION SECURITY

Application security overlaps with many of the topics covered in other chapters but needs to be considered as a separate security concern as well.

The aim of web application security is to identify the following:

- Critical assets of the organization
- Genuine users who may access the data
- The level of access provided to each user
- Various vulnerabilities that may exist in the application
- Data criticality and risk analysis on data exposure
- Appropriate remediation measures

Application security

- The use of software, hardware, and procedural solutions to protectapplications from external threats.
- This includes adding features or functionality to application software toprevent a range of different threats.
- It also includes security features outside the application, such as firewalls,antivirus software, and access control methods.

Business Application Register

- Application portfolio management, there should be an inventory, or register, of all applications, with details concerning the application, including security- related aspects.

TABLE 9.3 Information to Be Included in a Business Application Register

Category	Information
Type	▪ Developed in-house, **commercial-off-the-shelf (COTS) software**, cloud-based software, mobile-based software, end user-developed software
Operational	▪ Business purpose ▪ Business processes supported by the application
	▪ Relative importance to the organization (for example, critical, important, nonessential) ▪ Owner
Users	▪ Type and number of users ▪ Type and volume of connections
Access security	▪ Method of user authentication ▪ Network security barriers (for example, firewall, IPsec)
Type of data accessed	▪ Personally identifiable information ▪ Sensitive information (requires strong confidentiality) ▪ Requires strong availability ▪ Requires strong integrity
Technical	▪ Application version ▪ Supplier and licensing requirements ▪ Technical support contact

Commercial-off-the-shelf (COTS) software

- Software that is commercially available, leased, licensed, or sold to the general public and that requires no special modification or maintenance over the life cycle of the product to meet the needs of the procuring agency.

2.Business Application Protection

- The business assets, sound security architecture principles should beappliedto business applications.
- The considerations are somewhat different for two categories: *internallydeveloped applications and externally-developed applications*.

Internal Application Security

For any application that is developed within the organization, it is essential toincorporate security into all stages of the SDLC

- Document security requirements.
- Develop standardized procedures for evaluating application securityproducts and services.
- Enforce compliance with government and industry standards andregulations.
- Develop a policy for pre-deployment application testing and validation
- Construct a policy for documentation of application code review.

External Application Security

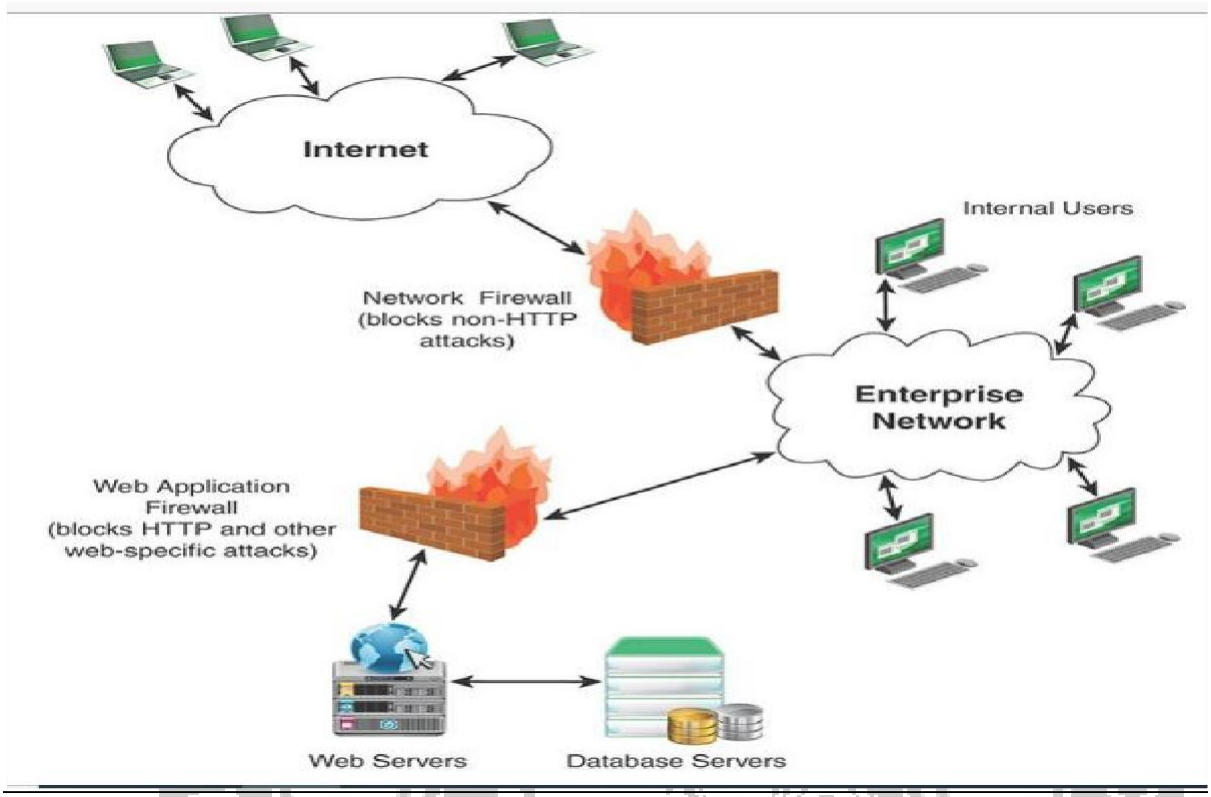
- The external environment, including the host operating system or virtual operating system, the hardware platform, and network connections
  - Protection against unauthorized access using access control measuresat the operating system level
  - Enforcement of virtual platform security
  - Encryption of network traffic using Transport Layer Security (TLS) orInternet Protocol Security (IPsec)

3. Browser-Based Application Protection

- As enterprises move applications online, both for internal use and for external users, such as customers and vendors, web application security becomes an increasing concern.
- Web Application Security Risks
  - Injection
  - Broken authentication
  - Sensitive data exposure
  - Security misconfiguration
  - XML external entity
  - Insecure deserialization
  - Broken access control
  - Using components with known vulnerabilities
  - Cross-site scripting (XSS)
  - Insufficient logging and monitoring

Web Application Firewall

- The most important tool in countering web application threats is a web application firewall (WAF), a firewall that monitors, filters, or blocks data packets as they travel to and from a web application.



Context for a Web Application Firewall

- There are a number of hosting options for WAFs, including the following:
  - Network-based
  - Local hardware:
  - Local software

Network-based:

- A network-based firewall is a hardware firewall incorporated with a router atthe edge of an enterprise network, acting as a filter to all traffic to and from network devices, including web-based application servers.
- Because there may be a variety of web applications on a number of servers, this approach can be complex to maintain. In addition, a network-based firewall may not be placed so as to catch internal traffic.

Local hardware:

- A local hardware firewall is placed between the application server and itsnetwork connection or connections.
- This type of firewall is much simpler than a network-based firewall because itonly has to have logic for filtering traffic specific to the local server.

Local software:

- A local software firewall is built on the server host operating system orvirtual machine operating system.
- This approach can be as effective as a local hardware firewall and is easier toconfigure and modify

Key features

- Real-time application security monitoring and access control:
- Virtual patching
- Full HTTP traffic logging
- Web application hardening

Real-time application security monitoring and access control:

- All HTTP traffic in both directions passes through Mod Security, where it can be inspected and filtered. Mod Security also has a persistent storage mechanism, which enables tracking of events over time to perform eventcorrelation.

Virtual patching:

- This is the ability to apply web application patching without making changes directly to the application.
- Virtual patching is applicable to applications that use any communication protocol, but it is particularly useful with HTTP because the traffic can generally be well understood by an intermediary device.

Full HTTP traffic logging:

- Web servers traditionally do very little when it comes to logging for security purposes. Mod Security gives you the ability to log events, including rawtransaction data, which is essential for forensics.
- In addition, the system manager gets to choose which transactions are logged,which parts of a transaction are logged, and which parts are sanitized.

Web application hardening:

This is a method of attack surface reduction in which the system manager selectively narrows down the HTTP features that will be accepted (for example, request methods, request headers, and content types).

Web Application Security Policy

- The European Union Agency for Network and Information Security (ENISA9).
  - Data Breach Investigations Report web application vulnerabilities accountfor the largest portion of attack vectors after malware.