E-Content of

INTERNET TECHNOLOGY AND WEB DESIGN

Chapter: 11.2 Overview of Internet Security

Topic: 11.2.1 Overview of Internet Security

Overview of Internet Security

- Internet is a vast world of several computers in a very large network.
- The three words 'vast', 'several' and 'very large' don't allow us to deny the importance of security in the field of data communication and networking.
- Internet security is used to protect websites and other electronic files from being attacked by hackers and viruses.
- Security concerns are in some ways peripheral to normal business working, but serve to highlight just how important it is that business users feel confident when using IT systems.
- Simply because cyber criminals know that a successful attack is very profitable and security will probably always be high on IT systems.
- Thus it means that cyber criminals will always strive hard to find new ways around IT security and users will consequently need to be continually vigilant.
- In the computer industry, Internet security refers to the techniques for ensuring the data stored in a computer cannot be read or compromised by any individuals without authorization.
- Most security measures involve data encryption and passwords.
- When computer connects to a network and begins communicating with others, it is taking a risk.
- Internet security involves the protection of a computer's internet account and files from intrusion of an unknown user.
- Basic security measures which involves protection by passwords (a secret word or phrase giving user access to system or a program), change of file permissions and back up of computer's data.
- Thus it is clear that whenever decisions are to be made about how to enhance a system, security will need to be held upper most among its requirements.

E-Content of
INTERNET TECHNOLOGY AND WEB DESIGN

Chapter: 11.2 Overview of Internet Security

Topic: 11.2.2 Aspects and need of security

Aspects and need of security

- The information security picture is changing and threats are expanding.
- Our business practices are being transformed and many security products are evolving.
- These changes must be a part of our strategic thinking for the future.

Changing threats and consequences

- The fight is not against "pranksters" any more, but well financed and highly motivated criminals.
- We still must protect against e-mailed viruses, but are now more concerned about web based malicious software, self-propagating worms, attacks on vulnerable applications.

Changing business needs

- The primary customers for electronic services are no longer state employees, but citizens, organizations and business partners.
- To provide these services, user concentrate valued information in large database linked to applications open to people all over the world.
- User must show close attention to server configuration, application security, system and application patches, authentication and authorization, malicious traffic and other things that may not have been big concerns before.

New tools and methods needed

- User still needs to filter out spam and e-mail viruses and install border protections.
- User must also filter out malicious websites, apply patches quickly, develop secure applications, lock down desktops, implement secure configurations and remove unnecessary services from servers, use strong authentication, train employees, isolate data stored and more.

Vendor products, services and pricing are changing

- There is a trend toward bundling security tools and requiring purchase of the bundle.
- Vendors are providing discounts when only their products are used, even when it is contrary to best practice, example, using two different antivirus vendor's products.
- Products which used for long years are no longer top performers.
- As product lines expand, support seems to decline and vendors push for long term contracts to lock customers in.
- There is little price competition, except with a large volume purchase.
- Vendors are getting better at identifying threats and quickly updating their products to stop them.
- Usually no clear best product or company surfaces and stays at the top.
- Core security products are becoming commodities with many customers changing products regularly, rather than staying with the same product year after year.

Security needs to be strategic

- Security is not an extra cost add-on.
- It must become part of the core service-delivery requirements.
- Expecting all agencies to learn about choose, implement, manage and maintain new security measures independently is inefficient and costly.
- User need to develop long-term strategies that accomplish goals and then figure out how to achieve them.
- Working collaboratively and strategically user can improve security, reduce workloads and save money.
- It may allow us to take advantage of opportunities that user cannot individually.