MALWARE

-Malicious software designed to get into a system without the user being alerted or consenting with malicious intent.

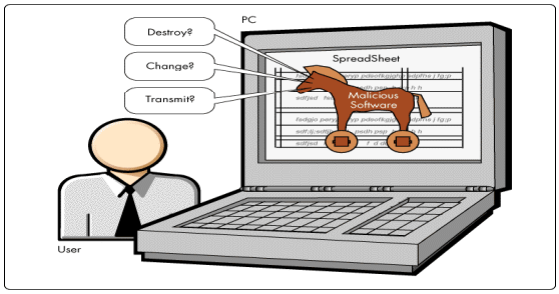
-No longer for only the privileged few.

MALWARE MITIGATION

-Keep Anti-virus products up to-date

-Users must exercise caution when opening e-mail and links in emails from un-trusted or unknown sources.

-Scanning of attachments entering your environment.



BOTS & BOTNETS

- A Bot is a computer that has been compromised by some type of malware allowing it's self to be remotely controlled by another source.

-A Botnet is a collection of Bots all under the command and control of a single entity.

DDoS ATTACKS

-DDoS occurs when a number of attacking host send numerous random communication request packets to a target IP address or address's

-Goal is to limit, disrupt, and prevent access to a network resource.

DDoS ATTACK

Some of the top reasons for a DDoS attack.

-Blackmail corporations for financial gain.
-Ideological differences
-Protesting
-Notoriety

DDoS MITIGATION

Best defense is to plan for it.

-ISP support to include contact information.
-All entities understanding actions required if an attack occurs.
-Prioritize source IP's or protocols that are essential.
-Disable any unneeded services on the environment.

DATA SECURITY

-Network hacked exposing over 100 millions credit card user's information.
-Lost hard disk containing information of over 15 million customers.
-Hard drive improperly disposed containing over 75 million personnel records.
-Over 15 thousand personal identities including Social Security numbers potentially compromised due to Malware infection.

DATA SECURITY

PROTECT and SECURE YOUR DATA.

-Provide end-to-end encryption from client to server, server to database, and database to disk or tape.

-Encryption of data at rest.

-Secure handling procedures

WEB BASED ATTACK

-Attack the application instead of the network.

-Basis of attack is to provide a normal or modified request that will exploit any poor parameter checking (XSS and XSRF).

-Wide spread growth of Web based attacks due to numerous application security vulnerabilities.

- Captcha breaking

WEB ATTACK MITIGATION

- Software architecture requires sound planning and oversight.

-Reverse web proxies.

FUTURE TRENDS

-Increased malicious activity from emerging Technology Countries.

-Mobile phones.

-Continued growth in the use of Malware.

REFERANCE

-Symantec. (2010). *Symantec Global Internet Security Threat Report.* Retrieved Aug 3, 2010 from http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf

-Sophos. (2010). *Sophos Security Threat Report: 2010*. Retrieved Aug 3, 2010 from http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jan-2010-wpna.pdf

-McAfee. (2009). *McAfee Threats Report: Third Quarter 2009*. Retrieved Aug 4, 2010 from. http://www.mcafee.com/us/local_content/reports/7315rpt_threat_1009.pdf

-CA. (2009). *State of the Internet 2009: A report on the Ever-Changing Threat Landscape*. Retrieved Aug 4, 2010 from. http://www.ca.com/files/SecurityAdvisorNews/2009threatreportfinalfinal_224176.pdf