Software Security Solutions for you and your organization.

By @jinankordab - softunivesum.com

Software solutions play a billion dollar role in some of today's environments. Although this paper discusses software security threats nowadays, I would like to point out to an incident that happened to stress the significance of Software and thus the significance of a *Secure* Software that should be taken in to a consideration during the development phase.

We all know Airbus. Couple of years ago Airbus was designing the largest airplane in the world (Airbus A-380), as a result teams in Germany, France (Toulouse), and England were developing different parts for the airplane. When the airplane was assembled, the testing phase showed a circuitry error between different parts. The teams reviewed their designs hundred of times, and found nothing. At the end they discovered that because *different teams used Different Software to do the task*, the parts didn't match. This cost the airline almost two billion dollars and a delay of almost two years, in which they lost some of their customers.

The transition from mainframe based systems computing to client-server architecture to global connectivity through internet has resulted in new computer security threats and challenges.

Security mechanisms for computer systems, either for standalone systems or networks, have been identified in theory, but in practice it is very hard to identify all security violations and threats that present a challenge to both software designers and clients.

Therefore, my short article will discuss major threats that are known to the digital age.

Threat One

Malicious Software (Viruses, Worms, Trojan Horses, Logical Bombs, Hackers Toolkit)

Advice:

Tell all employees to monitor their computers continuously, and check for unusual behavior, such as constant working of hard drive, or slow response time.

Solution:

Positioning combined security solution (antivirus and firewall and intrusion detection system "DOS Attack") at LAN Gateway to the Internet or other connected network. Thus the security of the whole network will be monitored at the entry point. It is advisable that this security solution uses "Deep Packet Inspection" technology, and be USB compatible device, which is very simple to install with no training costs, making sure that third party such as International Computer Security Association certifies it. Example: CP Secure, and SONICWALL. Antivirus and firewalls on standalone desktops are inadvisable due to the possible slow of performance.

Threat Two

Faulty Software and Poor System Administrator (Malfunctioning software, Software with bugs, Software with exploitable weakness "MS Outlook", some Open Source Software that can be reverse engineered decompiled, or debugged easily. Misconfigured Software such as Web Servers

Advice

Notify employees to contact someone in case of malfunctioning software or write a report exactly what happened.

Solution

Buy licensed software and keep updating it with new security patches once they are available from the vendor. Some companies offer free technical support for their products. Let the administrator configure access rights for employees and limit their executable rights, as well as access to some important software programs. Provide username and password login for each sensitive program.

For whatever browser is used to access the internet, provide Content Filtering by URL Blocking. Use *CyberNOT* filter that was adopted by organizations such as Microsoft, Netscape, AT&T, America Online, IBM, The Scolastic Network, because it is becoming the standard for implementing URL Blocking.

Threat Three

Insider threat by employees, or innocent employee mistakes and human errors such as :

- Staff member emails confidential documents to other companies
  Solution: Email scanning software, Corporate Security Policies

- An unauthorized internal user accesses confidential information by using a stolen password (example: password read off post-it note on the monitor)

  Solution: Corporate Security Policy

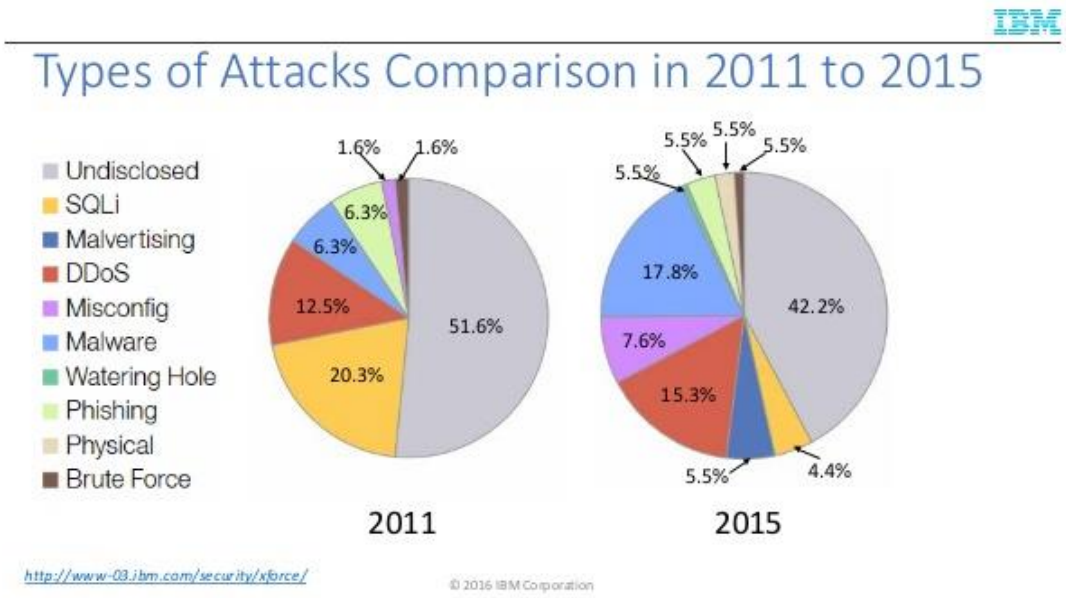
- Employee receives or downloads pornographic or other inappropriate content from the internet- reducing efficiency and exposing the manager to Legal Ability

  Solution: Internet and email scanning programs

- Employee error, or malicious act causes data to be destroyed or corrupted

  Solution: Tape Backup System

Statistics



CONCLUSION

If security was in mind while developing all software solutions, including Operating Systems, browsers, and standalone applications, it would be unnecessary to protect some software, computer, or networks later on. It is analogous to adding cement to sand, gravel and water to make a monolithic slab from three otherwise easily separable components.

Reference:

-**Malware beware [Real-time scanning keeps malicious code at bay]**

by Doug Beizer dbeizer@1105govinfo.com

- Home User Security: Your First Defense by Sarah Granger 2003-11-19

-Linux/Unix Security 101 by Payam Tarverdyan Chychi

-Transparent, Bridging Firewall Devices by Matthew Tanase 2003-10-15

-Zone Labs simplifies personal-firewall management (Simplified firewall management) By Wayne Rash , P.J. Connolly February 14, 2003

-Government of Canada Internet Guide http://www.tbs-sct.gc.ca/ig-gi/i-mo/sp/sp2_e.asp

-Firewall Evolution – Deep Packet Inspection by Ido Dubrawsky 2003-07-29 http://www.securityfocus.com/infocus/1716

-Threats to Computer Security – US Department of Commerce , http://alcor.concordia.ca/~helpline/security/threats.html

-Free BSD Handbook Chapter 29 Advanced Networking http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/network-bridging.html

-Virtual Private Networks for small to medium organizations, A White Paper by SonicWALL, Inc.

-Software Protection and Application Security:Understanding the Battleground? [A. Main P.C. van Oorschot]

1 Cloakware Corporation, Ottawa, Canada

2 Computer Science, Carleton University, Ottawa, Canada

-Cisco SAFE: Wireless LAN Security in Depth. A White Paper

Authors:

[Sean Convery (CCIE #4232), Darrin Miller (CCIE #6447), and Sri Sundaralingam ,Mark Doering, Pej Roshan, Stacey Albert, Bruce McMurdo,Jason Halpern]

-Local Area Network / Wide Area Network Security Threat Analysis

A Guide for Non-Technical Managers responsible for a corporate network

Copyright 2002 - Rick Macmurchie

-Wireless LAN Security: What Hackers Know That You Don't ,Kent Woodruff, www.airdefense.net

-White Paper,Why Organizations Choose CP Secure, www.cpsecure.com

- IBM Internet Security Systems Executive Brief, www.iss.net