Security, Risk and Compliance

The IBM Tivoli security strategy to face the current threat and vulnerability scenario

Pier Luigi Rotondo
Security IT Architect
IBM Italia S.p.A

IBM Service Management World Tour & Tivoli User Group

Roma, 20 ottobre 2008

Vulnerabilities' highlights [1]

- The overall number of vulnerabilities continued to rise as did the overall percentage of high risk vulnerabilities;
- The focus of endpoint exploitation has dramatically shifted from the operating system to the web browser and web applications;
  - Vulnerabilities affecting web applications are climbing and so are the attacks;
- For the first half of 2008, a *password stealer family* that targets online games is in first place on the top ten malware list;
  - One of the most common actions malware takes after installation is an attempt to evade detection, either by the user or by the security software on the system.

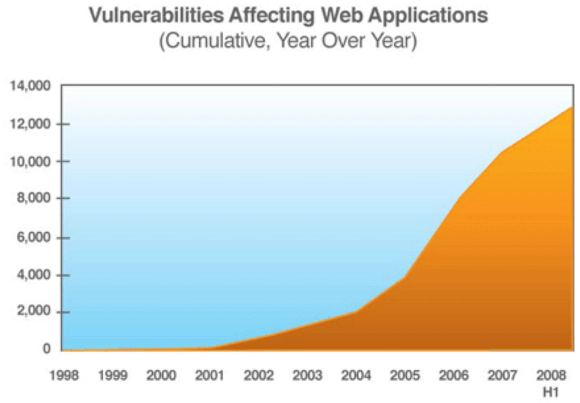
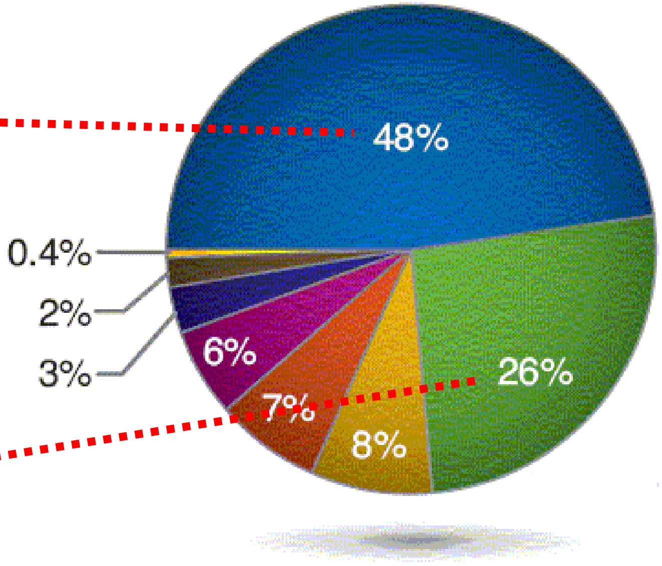


Figure 7: Cumulative Count of Web Application Vulnerabilities, 1998 – 2008 H1

© Copyright IBM Corporation 2008

Vulnerabilities' consequences [2]

- Gain Access (48%) - An attacker can obtain local and remote access
  - This also includes vulnerabilities in which an attacker can execute code or execute commands
- Data Manipulation (26%) - An attacker is able to manipulate data stored or used by the host associated with the service or application.

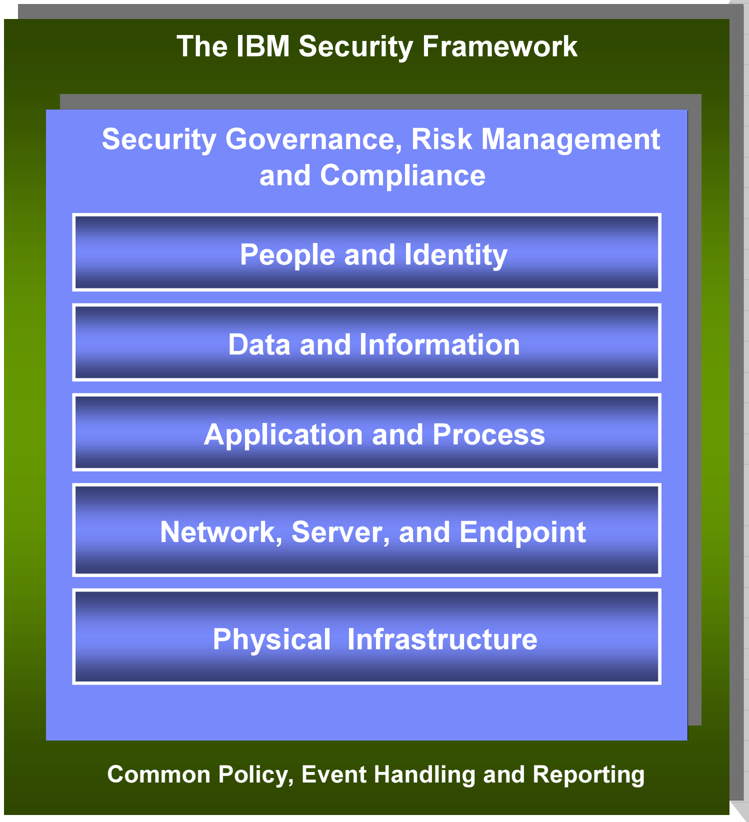


- Denial of Service (8%) - An attacker can crash or hang a service or system, or take down a network.
- Bypass Security (7%) - An attacker can bypass security restrictions such as a firewall or proxy, an IDS system or a virus scanner.

Attacks and information security incidents [3]

- The *most expensive* computer security incidents were those involving financial fraud, that account for only 12% of all the computer security incidents
  - At the same time the most common attacks are due to viruses, insider abuse, laptop theft
- Attacks that are targeting specific organizations or industry segments
  - Twenty-seven percent of those responding to a question regarding “targeted attacks” said they had detected at least one such attack.
- 51% of respondents did *not* report losses due to insiders

The IBM Security Framework


The IBM Security Framework
Security Governance, Risk Management and Compliance
People and Identity
Data and Information
Application and Process
Network, Server, and Endpoint
Physical Infrastructure
Common Policy, Event Handling and Reporting

SECURITY COMPLIANCE

- Demonstrable policy enforcement aligned to regulations, standards, laws, agreements (PCI, FISMA, etc..)

IDENTITY & ACCESS (IAM)

- Enable secure collaboration with internal and external users with controlled and secure access to information, applications and assets

DATA SECURITY

- Protect and secure your data and information assets

APPLICATION SECURITY

- Continuously manage, monitor and audit application security

INFRASTRUCTURE SECURITY

- Comprehensive threat and vulnerability management across networks, servers and end-points

References

1. *"IBM Internet Security Systems X-Force® 2008 Mid-Year Trend Statistics",* IBM Global Technology Services, July 2008 – available at http://www.ibm.com/services/us/iss/xforce/midyearreport/

2. *"IBM Internet Security Systems X-Force Threat Insight Monthly",* IBM Internet Security Systems, June 2008

3. R. Richardson, *"2008 CSI Computer Crime & Security Survey",* Computer Security Institute, October 2008

- All of IBM Tivoli Security Solutions are available at http://www.ibm.com/software/tivoli/solutions/security/