PATCHLINK™

Understanding the Five Ps of Security Patch & Vulnerability Management

Presented by
Peter Marini, Sales Director,
Australia and New Zealand
www.patchlink.com

Agenda

- The Vulnerability Picture
  - Hackers Around the World Turn Up The Heat
- Why is it so Painful?
- The "5 Ps"
- Summary / Q & A

Hackers Around the World Turn Up the Heat

The Current Threat Picture

- Sophisticated
- Focused
- Motivated by Money
- Motivated by Fanaticism
- It's More Than Just a Good Time

Exposure to Vulnerabilities

The Australian Computer Crime & Security Survey, May 2004:

- A large portion of surveyed respondents reported that virus, worm or Trojan infection was the core abuse during the prior 12 months

- 71% of respondents noted that these infections caused them financial loss

AusCERT
Australian Computer Emergency Response Team.

5

Gartner

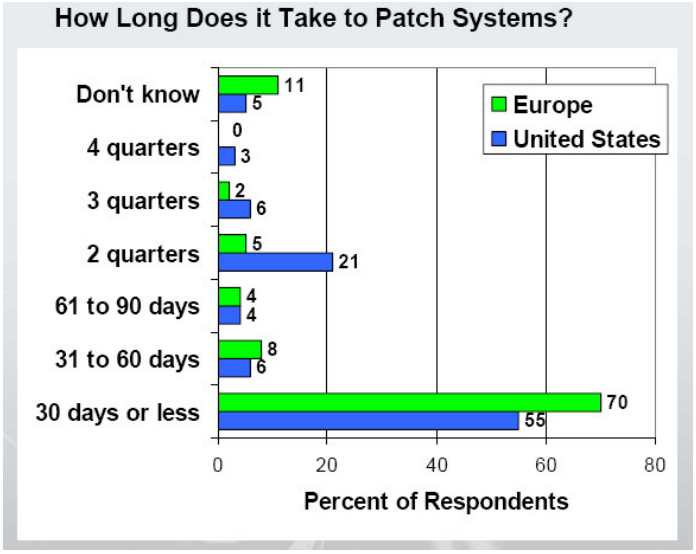
According to research firm Gartner in 2004:

<97% of security exploits are carried out through vulnerabilities for which there are known patches.

6

Why is Patching Painful?

Yankee



Source: The Yankee Group 2004 Enterprise Security Spending Survey

The Real Problems

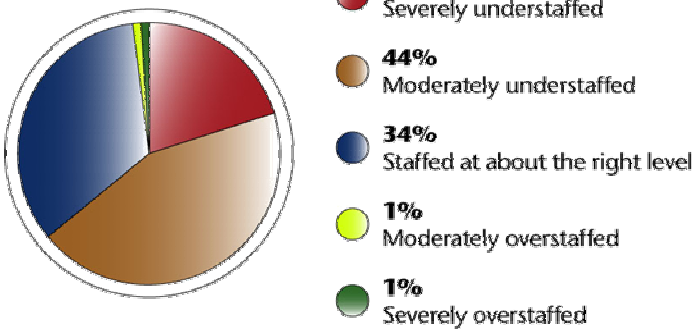
- Fragmented or departmental (and IT vs IT Security)
- Manual – time involved
- Disjointed efforts
- Blind / not tested or verified
- Buggy software

Out of Time

- Too many!
  - In 2004, CERT published 4,000+ security vulnerabilities
- Cost
  - According to Yankee Group:
    Can cost $100K's annually to manually deploy a single patch in a 1,000 node network
- Interval between vulnerability & exploit is shortening

Current IT Climate

Most InfoSec Organizations are Overwhelmed



Base = 1,395

Data: *Secure Enterprise* Security Deployment Survey, October 2004

11

The 5 Ps

12

Introducing the "5 Ps"

- The 5 Ps – a security maxim
  - Plan
  - Prioritise
  - Policy
  - Performance
  - Products
- The 5 Ps + patch & vulnerability management = an integral part of your overall security management strategy

1. Plan

- Planning involves:
  - An IT risk assessment: ***what*** are the potential vulnerabilities, ***where*** are they, and ***how*** critical?
  - The vulnerability status in each piece of firmware & software
  - Also establish which systems are critical, which should be patched first & which need constant maintenance

2. Prioritise

- Don't patch everything straight away
- Deal first with the systems that are most prone to attack or hacking – such as ecommerce & mail systems & critical business applications
- Then move to non-critical systems
- Maintenance in bite sizes
- Also factor in timing of maintenance

3. Policy

- Risk assessment + patching priorities = policy: what patches should be applied to which systems & in what order?
- Incorporate 2 elements:
  - one to deal with routine, non-critical patching issues in a regular, repeatable maintenance cycle
  - a second for serious patches installed quickly
- The policy should have procedure for assessing & distinguishing the severity of new alerts

4. Performance

- Q's to ask:
  - How big is the hole to be patched?
  - How severe is the risk to systems?
  - Does the patch require other system upgrades first?
- Test before applying patch
  - Use tools like Vmware to test in virtual environment
- Following a successful test, roll-out on trial basis, to limit risk
- Some patch & vulnerability management solution vendors will also test and authenticate patches before making them available helping to reduce your workload

5. Products

- The key points to check in any patch & vulnerability management solution are:
  - Are the patches secure & signed for authenticity?
  - Is the solution scalable?
  - Does the vendor test patches before shipping them, ensuring an additional level of reliability & stability?
  - Is there a patch library or repository?
  - Does it offer multi-platform support?
  - How granular is the management?
  - Can it group users & prioritise patch deployment?
  - Does the solution offer rollback capability, if a patch causes any issues?
  - Does the product assist with your processes?

A Strategic Response

- Security to Work Toward
  - An Extended Agency-wide Solution
  - Fully Automated & Integrated
  - Continuously Improving
  - Visible & Measurable

Summary

- Today IT threats are focused, sophisticated, on the rise, motivated by money & fanaticism
- There will always be patches to deploy & configurations to fix
- There are rational decision processes to employ
- Add the 5Ps to your overall security strategy


Large Business
Q&A
EPA
FAA
FDA
City of Boise
U.S. AIRFORCE
AFL-CIO
Gaithersburg
POLICE
LIBRARY
US Army Corps of Engineers
U.S. COURTS
NAVY
USDA
DOD
DOE
NASA
NRC
SEPA
DOT
Department of Veterans Affairs
VA
21