sollievo

Vulnerability Scanning and Patching

Agenda

- What is a vulnerability
- Where do they come from
- Why do we need to look for them
- How do we find them
- How do we verify they have been fixed

sollievo

What is a vulnerability

- The quality or state of being exposed to the possibility of being attacked or harmed, either physically or emotionally.

sollievo

Where do vulnerabilities come from???

- Hardware
  - Computer
  - Network Equipment
  - Processor Chips
- Software
  - Operating Systems
  - Websites
  - 3rd Party Applications

sollievo

Where do vulnerabilities come from???

- Unintended weaknesses in the development of the program or hardware.
- Some are never seen
- Some are unknown until…..

sollievo

sollievo

Vulnerability Scanning & Penetration Testing

Why do we scan for vulnerabilities???

- Because they are there…
- You cannot defend against what you don’t know about…
- Don’t be the Ostrich……

sollievo

Vulnerability Management

- According to SANS, vulnerability management is *the means of detecting, removing and controlling the inherent risk of vulnerabilities*

sollievo

Notable Breach - 2017

- Equifax

  - Announced September 7, 2017
  - 148 Million could be affected
  - Breach potentially occurred between mid-May and July of this year.
  - Discovered by Equifax on July 29 and announced September 7.
  - Cause – known vulnerability – notified by vendor to install patch, a lack of action by Equifax led to the breach.

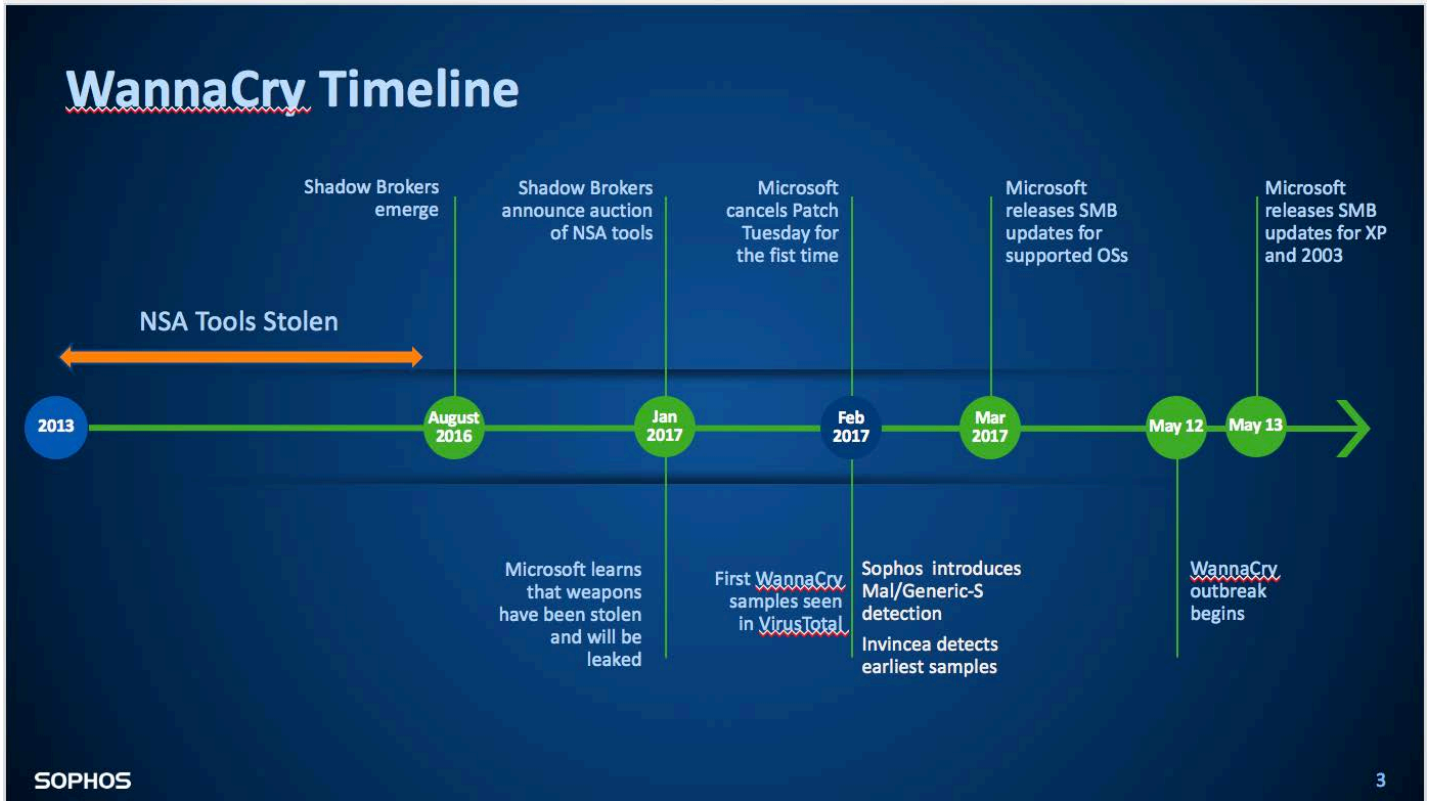
sollievo

Ransomware Attack - 2017

- WannaCry(pt) Ransomware
  - How Did It Happen?
    - Concerted attack exploiting a recently known Microsoft vulnerability
    - Microsoft patched the vulnerability in March
    - Delivery channel has varied
      - Email
      - Port scan
    - 300,000 systems
    - 150 countries

sollievo

WannaCrypt



sollievo

Vulnerability Scanning vs Penetration Testing

- Vulnerability Scanning:
  - Mechanism that scans network assets for known vulnerabilities and exploits.

- Penetration Testing:
  - Starts with a vulnerability scan, but takes it further by having someone (ethical hacker) try to exploit any discovered vulnerabilities.

sollievo

Vulnerability Scanning

- Considerations with Vulnerability Scanning
  - Scan Everything…
    - Hardware Inventory (Complete and Comprehensive)
  - Scan as often as possible…
    - But at least Quarterly
  - Have a process in place
    - Review reports
    - Evaluate/Prioritize the findings
    - Mitigate the vulnerabilities

sollievo

Penetration Testing

- Penetration Test
  - External Pen Test @ a minimum
  - Mature to External/Internal Testing
  - As thorough as possible
  - Beware of external vulnerability scans marketed as penetration tests
  - Have a process in place
    - Review reports
    - Evaluate/Prioritize the findings
    - Mitigate the vulnerabilities

sollievo

Additional Thoughts

- Wireless Penetration Test
  - Especially if the wireless network is not physically separated from your production network
- Authenticated Scans
- Separate Vendors
- In-House vs Vendor Service

sollievo

In-House Vulnerability Scanners

- Open VAS
- GFI LanGuard
- Nessus
- Nexpose

sollievo

Vulnerability Mitigation Steps

- Conduct regular vulnerability assessments
- Evaluate and prioritize findings
- Fix or mitigate findings
- Verify

sollievo

sollievo

Patching Process & Documentation

Patching

- Considerations when patching
  - All assets and software/applications
    - Hardware Inventory
    - Software Inventory
  - Have a process
    - How do you patch
    - Do you Test
    - When do you patch
    - Confirm patches have been installed

sollievo

3rd Party Applications

- Adobe
- Java
- Mobile Apps

sollievo

Patch Management Steps

- Conduct regular vulnerability assessments
- Test new patches
- Deploy new patches
- Verify

sollievo

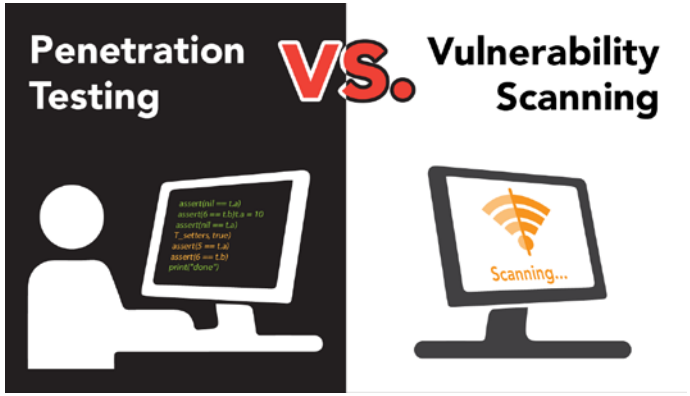
Documentation

- Document Everything
  - Inventory
  - Patching Policy / Standards
  - Vulnerability / Pen Testing Standards
  - Management / Board Reporting
    - Patching Results
    - Vulnerability Results (Penetration Tests)
    - Firewall Logs

sollievo

Vulnerability and Penetration Testing

- Final Thoughts on Vulnerability Scanning and Penetration Testing



sollievo

Patching

- Final Thoughts on Patching

sollievo

Closing Thoughts

- Regularly scheduled vulnerability scanning and a well-practiced patching program are two-halves of one whole solution to better protect you network and your Member's data.

sollievo

sollievo

Questions?

Contact Information

Mike Bechtel
Senior Consultant, Information Security Services
mbechtel@sollievo.com
Toll-Free (855) 605-5664
Phone (717) 985-5330 ext. 1101
Website: www.sollievo.com

sollievo