2005 NebraskaCert Conference

An Introduction to Automated Security Patch Management in the Enterprise Environment.

Jerry Errett, CISSP PMP

Overview

Automated Security Patch Management

- What is it?
- Why do you care?
- How do you do it?
- Things that make it hard.
- Things to Remember.

What is it?

Automated Security Patch Management

A process that manages the detection and remediation of software vulnerabilities to improve the security and integrity of a computer system.

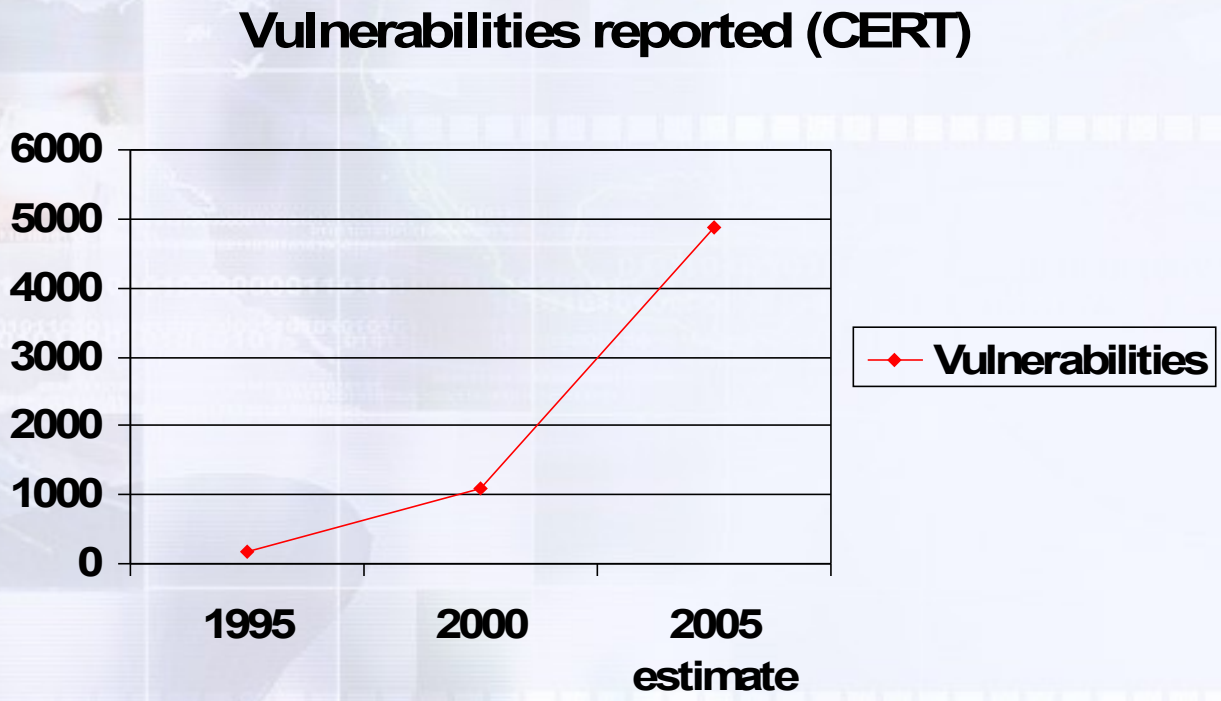
Overview

Automated Security Patch Management

- What is it?
- **Why do you care?**
  - **Cisco code theft**
  - **Card Systems Solutions**
  - **DSW**
- How do you do it?
- Things that make it hard.
- Things to Remember.

Why Do You Care?

You need Security Patch Management



Without it, security breaches can be catastrophic.

Why do you care?

Cisco Code Theft

- Code stolen in May 2004
- Thief used compromised SSH
- OpenSSH trojaned in Au
- Part of much larger atta

Why do you care?

CardSystems Solutions

“Inadequate security at credit card processor CardSystems Solutions Inc. is being blamed for a break-in that has exposed more than 40 million credit card accounts to potential theft. The company says the system compromise was discovered May 22, after a MasterCard inquiry into a wave of fraudulent transactions.”

(Source Netcraft)

Why do you care?

CardSystems Solutions

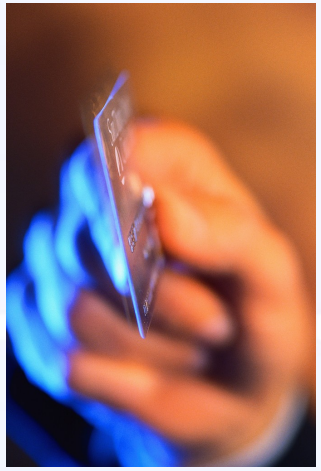
“MasterCard International said it, ‘worked with CardSystems to remediate the security vulnerabilities in the processor's systems. These vulnerabilities allowed an unauthorized individual to infiltrate their network and access the cardholder data.’ Officials at affected institutions were not specifying the vulnerability and exploit used to breach CardSystems' security.”

(Source Netcraft)

Why do you care?

“CardSystems, which processes more than $15 billion in transactions a year for 105,000 small businesses, said it ‘immediately began a remediation process to ensure all systems were secure,’ the company said in a statement. “

(Source Netcraft)



Why do you care?

DSW

- 1.4 million credit card numbers and names stolen. Theft detected in March 2005.
- Information taken from 108 stores, including the Shawnee Kansas store.
- Purchase information from Mid-November 2004 to Mid-Febuary 2005 included in theft.
- Mrs. Errett shopped at DSW shoes.

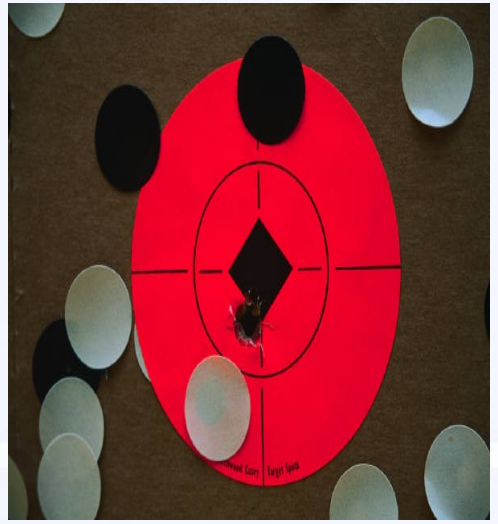
Overview

- What is “automated security patch management”?
- Why do you care?
- **How do you do it?**
  - Identify targets (Assets)
  - Determine vulnerabilities
  - Remediate
  - Repeat
- Things that make it hard.
- Things to Remember.

How do you do it?

Identify Targets

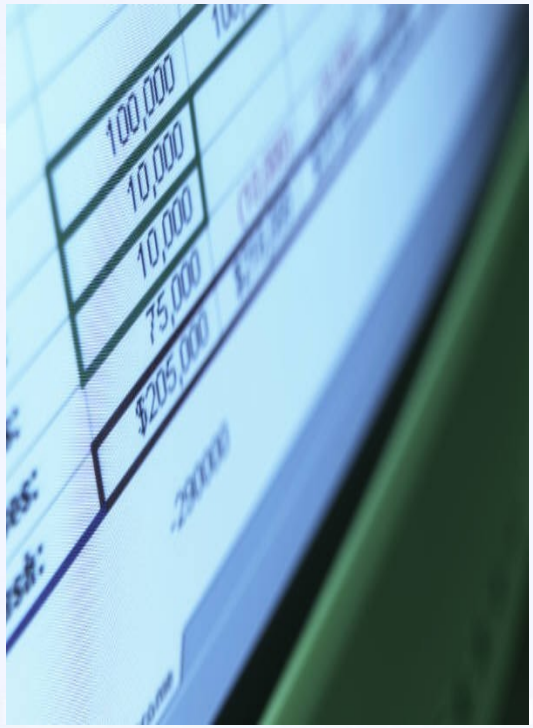
- Host based approach
  - Provides detailed information
  - Lower bandwidth
  - Requires agent installation
- Scanner based approach
  - Limited information
  - High bandwidth
  - No agent required



How do you do it?

Determine vulnerabilities

- Vulnerability information
  - Provided by vendor
  - Research
  - Provided by third party
- Platforms X applications
- Vulnerability information must be accurate and current.



How do you do it?

Remediate

- Prioritize remediation
- Determine remediation approach
- Package remediation
- Test remediation
- Perform remediation on targets
- Validate target vulnerability remediated

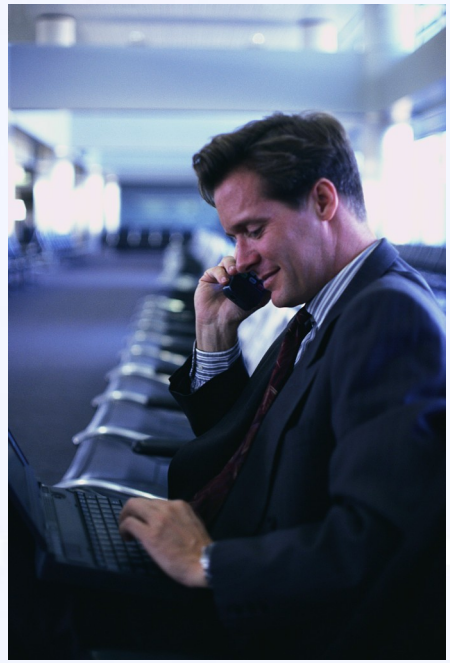
How do you do it?

Remediate

- **Prioritize remediation**
- Determine remediation approach
- Package remediation
- Test remediation
- Perform remediation on targets
- Validate target vulnerability remediated

How do you do it?

- Prioritize remediation
  - Vulnerability rating
    - Impact, Popularity, Simplicity
    - Exploit remotely, exploit locally
  - Asset protection (high, medium, low)



How do you do it?

Remediate

- Prioritize remediation
- **Determine remediation approach**
- Package remediation
- Test remediation
- Perform remediation on targets
- Validate target vulnerability remediated

How do you do it?

- Determine remediation approach
  - Remove or disable vulnerable software
  - Modify vulnerable software configuration
  - Patch vulnerable software
    - Single patch
    - Rollup patch
  - Accept risk

How do you do it?

Remediate

- Prioritize remediation
- Determine remediation approach
- **Package remediation**
- Test remediation
- Perform remediation on targets
- Validate target vulnerability remediated

How do you do it?

- Package remediation
  - Precise (dumb) remediation deployment package
  - Flexible (smart) remediation deployment package
  - Pre-requisites
  - Conflicts
  - Post-requisites
  - Multiple patches

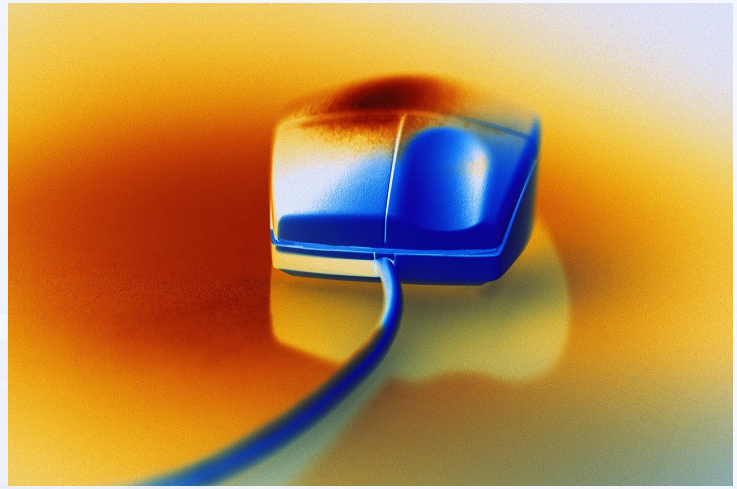
How do you do it?

Remediate

- Prioritize remediation
- Determine remediation approach
- Package remediation
- **Test remediation**
- Perform remediation on targets
- Validate target vulnerability remediated

How do you do it?

- Test remediation
  - Does asset function after remediation?
  - Result codes
  - Reboot required?
  - Package Type or Compression issues



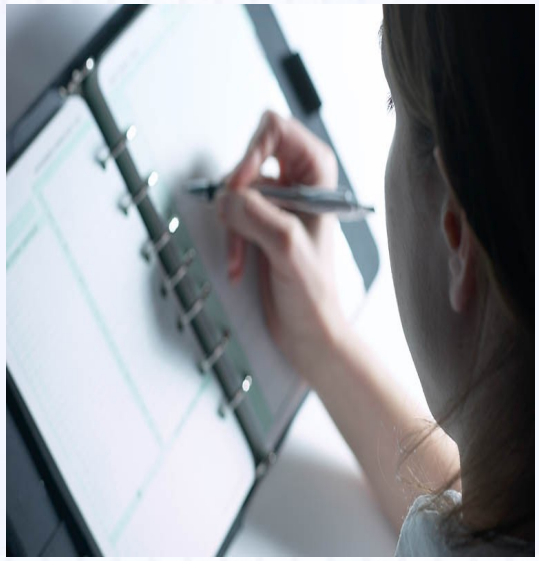
How do you do it?

Remediate

- Prioritize remediation
- Determine remediation approach
- Package remediation
- Test remediation
- **Perform remediation on targets**
- Validate target vulnerability remediated

How do you do it?

- Perform remediation on targets
  - Schedule deployment
  - Stage deployment
  - Minimize service outage



How do you do it?

Remediate

- Prioritize remediation
- Determine remediation approach
- Package remediation
- Test remediation
- Perform remediation on targets
- **Validate target vulnerability remediated**

How do you do it?

- **Validate target vulnerability remediated**
  - **Did remediation get applied?**
  - **Is vulnerability still detected?**

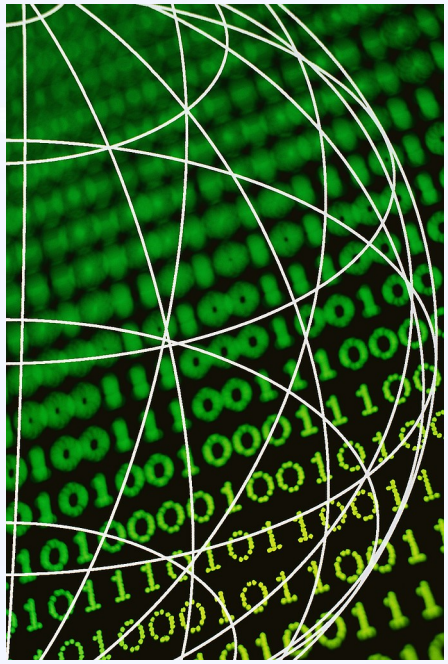
Overview

- What is “automated security patch management”?
- Why do you care?
- How do you do it?
- **Things that make it hard.**
- Things to Remember.

Things that Make it Hard

Difficult Areas Include:

- **Complex applications**
- **Multiple platforms**
- **Localization**
- **Time zones**
- **Corporate cultures**



Overview

- What is “automated security patch management”?
- Why do you care?
- How do you do it?
- Things that make it hard.
- **Things to Remember.**

Things to remember

- If you can patch it, you can break it!
- All bad guys are not outside the company.
- Sarbanes-Oxley
- Speed is critical, it is your best defence against zero day exploits.
- Vulnerability content is the most important ingredient.
- If you can’t test it, you shouldn’t patch it.
- Security information needs to be secured.

Things to Remember

links

- ca.com
- webappsec.org
- cert.org
- zone-h.org
- secunia.com
- frsirt.com

The end