Improve Security with Automated Patch Management

Mark Lillywhite
Introduction

• Security is a combination of protection, detection and response
• Good Systems Management enables Good Security
2014 – a memorable year

- Wirelurker – targets MAC OSX & iOS
- Poodle – killed SSLv3 / Heartbleed also
- Shellshock targets BASH
- JP Morgan hacked for 83 million records
- Backoff malware hits 1000’s retailers
- Sony comprehensively hacked
- 1000 banks in China / Uzbekistan hacked
Background

- SANS institute initiated contact with 1E in 2013
- SANS wants Microsoft SCCM as the infrastructure data source, as it’s used by over 65% of Organizations
- Too many other security solutions stand up separate infrastructures
SANS.org 20 Critical Security Controls

Version 5

1: Inventory of Authorized and Unauthorized Devices
2: Inventory of Authorized and Unauthorized Software
3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4: Continuous Vulnerability Assessment and Remediation
5: Malware Defenses
6: Application Software Security
7: Wireless Access Control
8: Data Recovery Capability
9: Security Skills Assessment and Appropriate Training to Fill Gaps
10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11: Limitation and Control of Network Ports, Protocols, and Services
12: Controlled Use of Administrative Privileges
13: Boundary Defense
14: Maintenance, Monitoring, and Analysis of Audit Logs
15: Controlled Access Based on the Need to Know
16: Account Monitoring and Control
17: Data Protection
18: Incident Response and Management
19: Secure Network Engineering
20: Penetration Tests and Red Team Exercises
SANS.org 20 Critical Security Controls

• As per SANS, effective implementation of four security best practices has been proven to mitigate more than 85% of cyber-attacks
Why bother?

- 80:20 rule
- Or the 99:1 rule
Four Control Benchmark

GOOD SECURITY IS GOOD SYSTEMS MANAGEMENT

Benchmark Against the Top 4 Controls
Provide an understanding of the top four controls that if implemented correctly stop at least 85% of cyber attacks.

Advanced Risk Analysis
Grades your environment from A-F based on the results of the information found in the environment.

Built-in help to improve your score
Provides recommendations to help improve the rating using 1E system management experience.

Leverage Existing infrastructure
SaaS model means no infrastructure or implementation costs, no agent needs to be installed on the end points.

At least 85% of the intrusions that ASD responded to in 2011 involved adversaries using unsophisticated techniques that would have been mitigated by implementing the top four mitigation strategies. Australian Signals Directorate, February 2014
Four Security Controls

- **Operating System Patching**
  - Measure how up to date Operating Systems are across the entire estate.
  - Done by combination of the updates coverage across the estate as well as time from when the updates are made available to when they are applied.

- **Application Updates**
  - Measure how up to date applications are across the entire estate.
  - Done by combination of the updates coverage across the estate as well as time from when the updates are made available to when they are applied.

- **Restriction of Administrative Privileges**
  - Evaluates local group membership and domain members for systems in the estate and calculates how well limiting administrative access is being controlled.

- **Application Whitelisting**
  - Computer administration practice to prevent unauthorized programs from running.
  - Measures the effectiveness of the whitelist implementation.
  - If no whitelisting implemented, it evaluates the Risk Profile.
1E Security Benchmarking Dashboard

Security Compliance

Grade

F

Grade Calculation

Control Maturity

Whitelisting

Control not implemented

Control Maturity

OS Updates

53

Control Maturity

Application Updates

73

Control Maturity

Administrative Privileges

Control data not available

About Dashboard

This benchmark measures your environment against four critical controls governed to mitigate 85% of cyber security threats. A maturity score is calculated for each control, these are combined into a benchmark rank A to F.

Application Updates Security Control Details:

Control Maturity

Application Updates

73

Information:

Control Information:

Coverage of Microsoft & Partner Application Updates: 62%

Microsoft update Deployments within an acceptable timeframe: 70%

Application installation update coverage: 94%

Measurement of third party (non-Microsoft) applications installed at the most recent version of available releases. When Emily sync is enabled, the coverage is calculated using the ActiveSync benchmark process, otherwise we use the highest available versions in your estate.

Application fix update coverage: 53%

Recommendations:

Implement best Practices

To ensure your estate by applying latest available Application Updates, follow the best practices outlined:

More Details
How does 1E Help with Patching

• 1E Nomad for acceleration of patch cycles
• 1E Wakeup for 802.1x compliant wakeup
• 1E Security Benchmark for peer comparison

**US Department of State**
The 1E WakeUp agent enables workstations to be powered on for patching, scanning (security, ConfigMgr, patch, virus, etc.), and software installation. These tasks are performed during non-business hours.

**Global Finance Company**
We have many offices globally and were suffering huge bandwidth issues. Being so very challenged in doing the day-to-day patching via our network was the main driver for investing in 1E Nomad.
How does 1E help with Admin rights

- It's all about give and take
- If you remove rights......
- You need to automate users getting things quickly

1E Shopping provides a single portal for all software and services...
Application Whitelisting

- Microsoft provide AppLocker
- 1E specialize in tools to enhance Microsoft functionality
- Watch this space ....
Top additional Recommendations

- Revoke admin rights or time them out
- Change of Role – prompt rights audit
- Define Incident response process / team
Who is 1E?

- 1E’s mission is to automate the Software Lifecycle
- Automation = Cost benefits
- Standardization = Security Benefits
Thank You for Attending the Webinar

Speaker: Mark Lillywhite, Mark.Lillywhite@1e.com

Subscribe to 1E Security Blogs

Register to participate in the Security Benchmark Beta Program

To learn more about the 1E solutions presented in this webinar
• Nomad
• NightWatchman

Upcoming 1E events and webinars
Software Lifecycle Automation

LEAN
Remove Software Sprawl
Optimal Licensing Strategy
ISO 19770 Process Compliance

SECURE
Four Controls Benchmark
Patch Management
Power Management

RESPONSIVE
Simple & Seamless Self-Service
On-Demand Windows Migration
Anywhere, Anytime BYOPC

FAST
Automated Endpoint
Server Reduction
Business Prioritized Network