WOLF
& COMPANY, P.C.

FMS Financial Managers Society

Stepping Up Your Cybersecurity Management

September 9, 2019

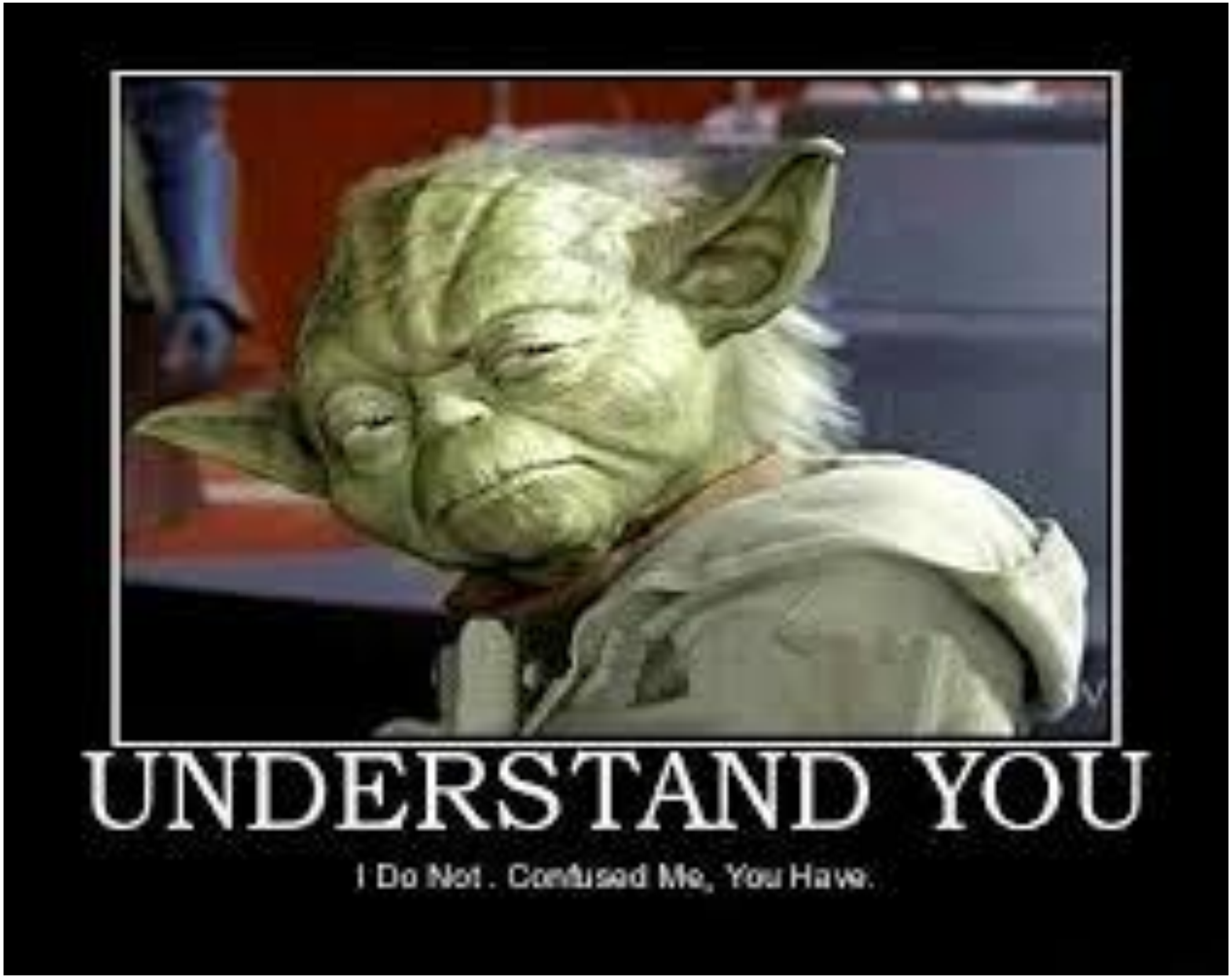
#1: Mismanagement of Assets

- Unable to identify what is connected to your network
- Unable to detect or prevent unauthorized software from running
- Hardware and Software inventories not accurate
- Unsupported systems running in the environment

Solution: Hardware and Software Inventories

- Maintain Detailed Hardware Asset Inventory
  - Utilize active and passive discovery tools
  - Use DHCP logging
- Deploy Port Level Access Control (such as a NAC)
- Use client certificates to authenticate hardware assets
- Maintain Detailed Software Inventories
- Ensure software is supported (i.e. end of life)
- Only allow authorized software to run (application whitelisting)
- Remove unauthorized hardware and software

#2: VA vs PT



Vulnerability Scanning

Pros

- Can be automated / scheduled
- Easily test all objects connected to your network

Cons

- Prone to giving false positives
- Hard to prioritize remediation efforts (volume)
- Categorize as low risk, but is it?

Penetration Testing

Pros

- Confirms exposure
- Find more granular issues that a vulnerability scan may not detect
- Can verify your detection and response capabilities (more on this later!)

Cons

- Manual, typically more expensive
- Testing may not hit every object (focus is sometimes limited)

Solution: Do Both!

#3: Vulnerability Management

- Not tied into your software and hardware inventories
- Not frequent enough or does not align with your patching process
- Too frequent and/or lack of resources to address issues identified in report
- Untrusted or non-credentialed scan
- Missing policies (frequency, risk ratings, etc.)

Solution: Vulnerability Scanning Process & Configuration

- Include all hardware and software objects
- **Align timing of vulnerability scanning with patch process**
- Provide resources to manage vulnerability scan data
- Implement governance process to measure results against policies
- **Perform a trusted or credentialed scan**
- Define your policies and patch moderate and lower risk vulnerabilities (as applicable)
- Deploy automated patch tools
- Measure your effectiveness (metrics)

#4: Pentesting Bang for Your Buck!

- Quality of your pen testers (rely on vulnerability tools)
- Not verifying your detective and response capabilities
- Limit scope and time

Solution: Pentesting

- Make sure you are getting quality pentesters
- **Include testing your detection capabilities**
- Give them enough time to do a thorough pentest
- Include all types of penetration testing:
  - Internal network
  - External network
  - Web application
  - Wireless
- Schedule different scenarios as you mature (have a multi-year plan approach)

#5: Administrative Access

- Misuse of administrator privileges is a primary method bad actors use
- Only “IT has admin access to the network” is not good enough
- Local administrator user accounts (i.e. workstations) all have the same password
- Not using a multifactor authentication
- Lack of basic monitoring

Solution: Locking Down Admin Access

- Maintain an inventory of administrative user accounts (use automated tools)
- Change defaults
- Use dedicated admin accounts
- Use unique passwords (i.e. local administrator accounts)
- **Use MFA**
- Use a dedicated workstation for all administrator task
- Limit access to scripting tools (i.e. Powershell)
- Log and alert of changes to group membership and on unsuccessful login

#6: Weak Configurations

- Default configurations
- Open services and ports
- Vulnerable protocols
- Unnecessary software running

“Our domain configuration is locked down using group policy (GPO’s) from Active Directory. We push out our configuration that way”

Solution: Strong Configurations

- Maintain a standard security configuration for all authorized operating systems and software
- Deploy system configuration management tools to enforce configurations
- **Implement system configuration monitoring systems**
- Maintain secure images and securely store master images

CIS Benchmarks™

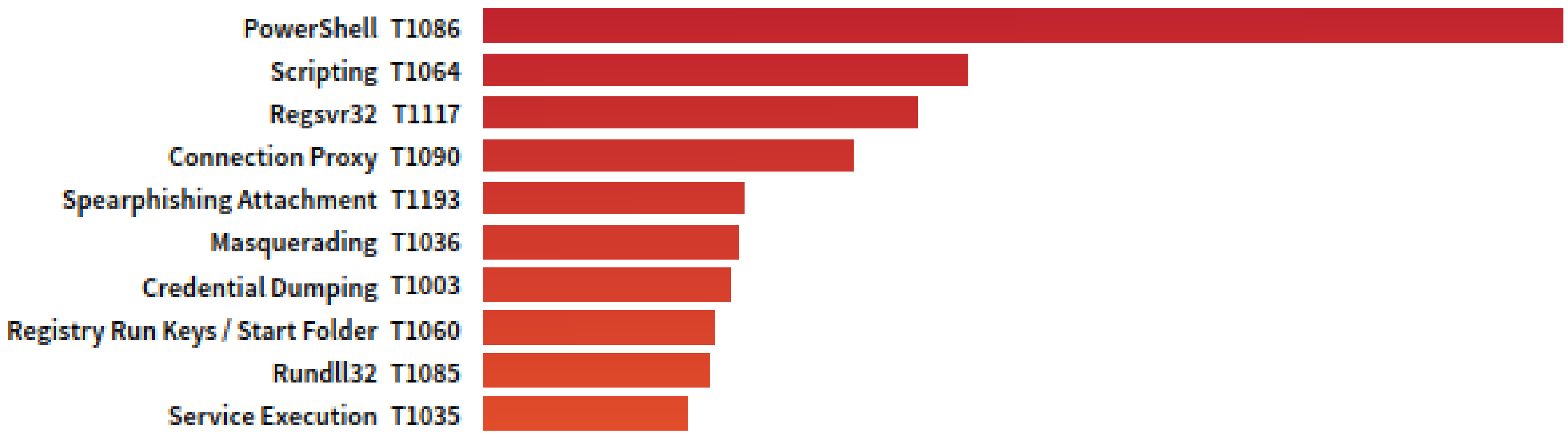
IASE Information Assurance Support Environment

#7: You're Blind to Activities

- Lack of centralization and correlation of logs
- Log collection scope is limited
- Monitoring systems (i.e. SIEMs) are not being managed
- Device clocks are different
- Logs are not properly analyzed to detect bad actors' activities

Solution: Implement a SIEM

- Activate audit logging
- Collect logs from all sources
- Utilize three synchronized time sources
- Centralized and correlate logs
- **Configure and management SIEM**



#8: Shiny Objects

- Purchasing that next generation technology
  - Lack of expertise
  - Lack of people resources
  - No process in place

Solution: Cybersecurity Strategy

- Understand your threats
- Understand your current profile
- **Define where you want to be (cybersecurity strategy)**
- Develop corrective action plans (in house or outsource)
- Measure and monitor progress

Know Your Enemy And Know Yourself And You Will Always Be Victorious.

"Sun Tzu"

Cybersecurity Trends

- Multifactor authentication for internal network
- Next generation malware protection (behavior based)
- Centralized logging and alerting
- Integrating threat intelligence into security systems
- Emulating phishing attacks (performed by in-house personnel) with increase frequency
- Secure configuration (patch management is only half of it!)
- Security Assessments
- Integrating cyber into ERM

Cybersecurity Trends

- Additional FTE’s both at the second line of defense and the first line of defense
- Use of additional security control frameworks
- Outsourcing missing expertise
  - Centralized logging and alerting / Security Operations Center
  - Integrating threat intelligence into security systems
  - Chief Information Security Officer / Information Security Officer (CISO/ISO) role
  - Incident response management (check your cyber insurance policy)

Conclusion: Do the Basics Well

- Know what is connected to you network
- Know what is running on your network
- Identify vulnerabilities, remediate, and minimize the window of opportunity for attackers
- Control admin privileges
- Secure configuration
- Maintain, monitor and analyze activity

Thank You!

William Nowik, CISA, CISSP, QSA, PCIP, CCSFP
Principal - IT Assurance Services
Phone: (617) 428-5469
Email: wnowik@wolfandco.com
LinkedIn: wnowik

www.wolfandco.com
www.wolfpacsolutions.com

References

- FFIEC Cybersecurity guidance
  - http://www.ffiec.gov/cybersecurity.htm
- NIST CSF
  - http://www.nist.gov/cyberframework/
- CIS CSC
  - https://www.cisecurity.org/controls/
- NIST SP 800-63 –
  - https://pages.nist.gov/800-63-3/
- Red Canary Threat Detection Report