BCNET

Shared IT Services for Higher Education & Research

Conference 2017

Setting up an Information Security Program

on a shoestring budget

Andy Scott, CISSP, GMON

Muhammad Noman Muneer

Approach

- Risk-based – it drives the security program
- Allow for quick wins and constant improvement
- Don’t make IT look bad – security needs friends
- Report on successes and opportunities for improvements

Roadmap

1. Assess organizations' risk tolerance and what is important to them
2. Set your target environment based on the risk tolerance
3. Perform a gap analysis
4. Prioritize recommendations and create implementation plan based on gap analysis
5. Mature and measure the information security program on an ongoing basis

Risk Tolerance

- Ask Senior Management and Board what their acceptable level of risk is
- Sometimes hard to get a good answer - ask, “What don’t you want to see on the front page of the paper?”
- Tie risk tolerance to the mission and vision statements. Here is a good place to start:
  - Institutions reputation
  - the learning environment
  - the systems that support the learning environment
  - the privacy of personal information that is collected

Setting your target environment

- Choose a framework (gives you a target and a way to measure your progress). Customize to match organization risk tolerance
- Recommend starting with 20 Critical Security Controls (quick wins and helps prioritize)
  - Design and configure your network and systems to ensure appropriate levels of security.
  - Keep systems and devices updated with the latest security patches.
  - Ensure access is limited to what is required.
  - Monitor controls and systems and investigate anomalies.

Gap analysis

- Do a black-box pen-test
- Go through framework and document where controls are sufficient and where they are lacking
- Check for policies / procedures, information classification
- Determine if there is Information Security governance

Gap analysis tools

- Google (reconnaissance), ssllabs, haveibeenpwned
- Nmap
- Nessus
- Kali including metasploit
- Auditscripts.com – tools for assessing 20 critical controls

Prioritize recommendations and create implementation plan

- Recommendations from gap analysis
- Group recommendations into larger categories (Use the categories identified in risk tolerance).
- Prioritize recommendations and focus on the Critical and High ones (biggest to smallest risk exposure)
- Create professional report with implementation plan and present to CIO and governance body

Mature security program & measure

- Implement tools to determine what is going on inside the network
- Constantly customize tools as discover new items to look for
- Continue applying security framework
- Establish a security awareness program (people are becoming easier to target than systems)

On to the good stuff …

SIEM to monitor for security events

- Snare Open Source Agent
- Dedicated syslog server (syslogd –r)
- Awk commands to parse the data (extract event id's and totals)
  - Awk –F"\t" '{print $7}' userlog.`date +%Y-%m-%d` | sort | uniq –c | sort –rn

Intrusion Detection (IDS)

- Security Onion OS (Host for Bro)
- Dedicated server with two NICs
- Network TAP / Spanned port

Automating event processing on Windows

- Outlook
- Powershell ISE
- ```
  #Create Outlook object using the API
  Add-Type -AssemblyName "Microsoft.Office.Interop.Outlook"
  $Outlook = New-Object -ComObject Outlook.Application
  $namespace = $Outlook.GetNameSpace("MAPI")
  ```
  ```

- Thank you!