MCNC

NCREN
NORTH CAROLINA RESEARCH AND EDUCATION NETWORK

Security Best Practices for grades K-12

Connecting North Carolina's Future Today

Overview of Security Issues

- Security as a process and NOT a technology.
  - Point solutions
  - Integration challenges
  - Lack of policies and procedures
- Time - Oh! BTW…
  - In addition to your regular duties…
- People
  - Users
    - No matter how many times you tell them…
  - Inquisitive kids with nothing better to do. (Me)

Overview of Security Issues

- Let’s talk about the Security Universe
  - Fortune 500
  - Government
  - Education
- Targets
  - Money
  - Intellectual Property
  - Additional drones for the DDoS Army
  - Personally identifiable information
  - Reputation
  - Changing grades or finding test answers… ☺

The Security Universe – Potential Issues

- Wireless Encryption
- Firewall Rules
- Remote Administration
- Patch Management
- Authentication
- Change Management
- Extraneous Services
- Network Management
- Weak Passwords
- Exposed Administration Interfaces
- Poor Coding Practices
- Anti-Virus
- Backups
- Intrusion Detection
- Logging Management
- Secure Builds
- Web Filtering
- Periodic Assessments
- Network Traffic Review
- Default Installations of Software

Good News and Bad News

- Bad News
  - You face the same challenges that every corporation, municipality, State and other organizations do.
  - You have do to it with less money and less people.
  - Budget Cuts
- Good News
  - By taking care of low hanging fruit, you can:
    - increase organizational security
    - make other targets seem easier to attack.
- No Security is foolproof – so let’s make your organization more difficult to attack, relative to others.

Policies

- Policies are the foundation upon which all security is built.
- Most policies, if existent, rarely contain correct elements.
  - Leave out enforcement provisions or cannot be enforced.
  - Some haven’t yet been written in the face of changing technology trends.
- Example policies that need your attention:
  - Password Policy
  - Data Classification Policy (Data Life Cycle)
  - Acceptable Encryption
  - Termination (Separation and Emergency)
  - Acceptable Use Policy
  - Remote Access Policy
  - Peer to Peer Policy

Perimeter Security

- Firewalls and Virtual Private Networks provide the basis for your perimeter security.
- Some best practices to follow when deploying:
  - Begin with a default DENY ALL rule.
  - Think of your rule set as a triangle with the most specific rules towards the top.
  - Ensure that ONLY services that are absolutely needed are allowed and only to the required destinations. (Source, Service, Destination)
  - Ensure that all default passwords have been changed
  - Ensure that anti-spoofing rules are enabled on each interface
  - Conduct periodic assessments of your network perimeter.
  - Ensure that only accepted encryption ciphers are being used.
  - Do not allow MS SMB ports through your perimeter firewall (135-139, 445) unless they are over an encrypted and authenticated tunnel.

Wireless Encryption

- The Evolution of 802.11i: WEP > WPA/TKIP > WPA2/AES
  - WEP/WPA fundamentally broken due to choice of cipher
  - http://www.wpacracker.com/
    - 284 million words
    - $17 & 20 minutes
- How do we fix this? Authentication.
  - Pre-Shared Key (PSK) vs. Dynamic Keys
    - PSK – Designed for SMB, SOHO (scaling issues in large organizations)
    - Dynamic Keys – initial password combined with a random IV. Key changes and key management are handled within the wireless transmission.
- PSKs in a large environment should be avoided where possible.
- The use of integrated authentication (RADIUS, 802.1x, AD, LDAP) helps to alleviate these issues.
- The minimum acceptable encryption should be AES-128 if your infrastructure supports it. Otherwise, 3DES.
- Also, for Hot Spots or Guest Networks, place them on a completely separate SSID and VLAN.
  - Do not allow them access to your internal network.
  - Offer only discrete services (e.g. HTTP, HTTPS, DNS)

Patch Management

- This is singularly the biggest issue we run across. Why?
  - It's like the US Mail, it keeps coming
  - Requires testing and outages
  - Frankly, it's boring work
- It is one of the two simplest ways to dramatically increase your security.
  - An attacker needs but to find a single vulnerability or missing patch to exploit.
- There are some tools available to check patch levels, but you generally get what you pay for.
  - Shavlik
  - BigFix
  - Altiris
  - ZenWorks
  - WMI – free, but requires Win32 scripting knowledge.
  - PERL – free, www.cpan.org
- Most effective Patch Management programs have fixed outage windows.
  - Many try to align with the DPI calendar

Passwords & Authentication

- This is the other “easiest” method to increase security in the environment.
  - Samples show that most LEAs have weak password policies (5 chars, no complexity)
    - Done for younger children (and Administrators)
- Integrated Authentication
  - Where possible, you should be using AAA services for your authentication.
  - RADIUS, AD, LDAP, Kerberos should be used in place of clear text protocols.
  - 2-Factor Authentication (e.g. RSA) for critical systems and remote access should be considered.
- Password complexity should be mandated where possible.
  - You can put Primary students in a separate OU if needed.
- A method for changing passwords to Service or SYSTEM accounts needs to be well thought out.

Logging Management & Review

- We have yet to see any LEA do this, properly or otherwise.
  - Don’t feel bad, most Fortune 500 don’t either.
  - Logs are the most valuable source of troubleshooting information.
- Volumes of information to sift through (Server logs, router logs, VPN logs, AV Logs, firewall logs, etc.) “Drowning in Information”
  - Time consuming
  - Lack of Disk Space
  - Lack of Comprehension – have YOU been trained on what Error 1747 is?
- Consider centralized log aggregation and correlation
  - Log Logic
  - Nitro Security
  - Arcsight
- 3rd Party Logging Aggregation and Management

Periodic Assessments

- "That which is not measured never gets managed."
- Periodic Assessments benefit the organization:
  - Show where potential risks may reside
  - Help in justifying budget and spend
    - Technology
    - Personnel
  - Shows due diligence and due care with respect to system, student and employee data.
- Assessments can be done in house with freely available tools.
  - Recommended to have an external source provide a yearly vulnerability assessment.
    - Different methodologies
    - Different and Proprietary tools
    - Core competency

Summary

- Securing your enterprise is a tough job. Lack of personnel and technology.
- Balance security and usability. Make your organization tougher than the next guy.
- Ensure that your security begins with policies and security awareness among your users.
- When deploying firewalls, ALWAYS start with a default DENY ALL rule and build from there. “SSD”
- Strong passwords, authentication and AAA services will help to reduce the risks in the organization.
- Patch Management is the most overlooked, but arguably the most important part of keeping the enterprise secure.
- Centralized Log Management and Correlation is becoming a must for the organization.
- Conduct Periodic self-assessments and 3rd Party assessments at least once a year.

Contact Information

- Jay Ward –WireGhost Security
  - jay@wireghost.com
- Dave Furiness–MCNC
  - dfurines@mcnc.org