What Does Your School District Need to Do?

MATT MCMAHON, GRATIOT ISABELLA RESA
JIM RARUS, WAYNE RESA
RYAN VELZY, OAKLAND SCHOOLS
Topics

• Cybersecurity workgroup – METL Initiative
  • Twenty critical security controls
  • What are the top six

• Social Engineering Prevention at Wayne RESA

• Securing Access at Oakland Schools
1. Inventory and Control of Hardware Assets

Executive Summary

IT Managers need to know what devices are on their network and where they are. Students and staff expect schools to support mobile personal devices, wireless networks and remote access. Each device on the network is a potential inroad for a security issue. IT Managers need to be able to locate and control access for any device currently attached to their network. Schools need to make access to their network convenient but also secure.

Network managers need to be able to quickly locate all devices on a network. This is typically done by referencing MAC addresses. Network administrators should regularly update and monitor DHCP logs. IT managers should be able to identify devices connected to the network. More sophisticated tools such as Netdisco and Lantopolog can be used to maintain historical logs of network changes.

Network managers should be able to identify and access only those devices with permissions to access the network. Hot ports should be removed and moved to the guest network. Wireless networks need to be created to allow guest access but not full access to network resources.

Case Study: All users at Example Schools connect their personal device, statically assigns the device the IP address of the network gateway which breaks Internet access for everyone. Using “show ip arp” on the router, the network administrator is able to locate the MAC address of the user. Using “show mac-address” on the switch, they are able to locate the specific port the user is connected to and disable it.

Getting Started

Netdisco: http://netdisco.org/
Lantopolog: https://www.lantopolog.com/
Locating a device on your network:
http://poxnet.linux/post/2010/06/18/locating-host-port-ip-address/
Relevant NEOLA Policy: 5136 - Wireless Communication Devices
Relevant NEOLA Policy: 7543 - Remote Access To The District’s Network

METL / Misen / Merit
1: Hardware Inventory

Do you know what devices are on your network?
Can you locate a user device during/after an incident?
Has “Internet of Things” crept in?
2: Software Inventory

What programs are installed - and where?

How are updates managed?

Is everything still supported?

What’s hiding in the closet?
3: Software Vulnerability Management

Are you being notified of new vulnerabilities?
... for everything?
Are you doing something about them?
Do you have a set maintenance window?
4: Control Admin Privileges

Who has the access to the Admin/root login?

Limit who, when and where

Do users work as administrator on their computers?
5: Secure Device Configurations

Are you using the default configurations?
Are you turning off unneeded services?
How are you managing mobile devices?
Can you push out changes quickly?
6: Log files

You’ve got ‘em - what are you doing with ‘em?

Are your devices synced to a single time source?

Gather log files onto one machine

Automate scans & reports
Social Engineering Explained

• The art of manipulating, influencing, or deceiving you in order to gain control over your computer system

• Old concept applied to information systems

• Hard to prevent through technology as it exploits human nature

• Reviewing e-mail phishing but many other avenues of deceit
  • On-site visits in uniform with a clipboard
  • Phone/Vishing (altered caller ID – Microsoft or IRS are examples)
Phishing – a form of Social Engineering

- E-mail from a “trusted source”

Recent examples – employee payroll change requests

Massive increase in reports over the last several months

Most likely all of you have heard of or been personally affected by such an e-mail

Example from MC3 01-14-19 alert
It is easy to be fooled

- More e-mail read on cell phones in haste
- Full e-mail addresses not displayed

Domain name not shown unless “>“ clicked
**Protection from staff name** Hijack

- Add a banner to all e-mail coming from the Internet
  - Powerful attention-getter
  - Genesee ISD example:
    - CAUTION: This e-mail originated from outside of Wayne RESA. Do not click links or open attachments unless you are expecting this e-mail and have verified the sender's authenticity.
  - Plante Moran example:
    - CAUTION: This email was sent to Plante Moran from an external source. Please be extra vigilant when opening attachments or clicking links
  - Wayne RESA “protects” Superintendent and Deputy Superintendent e-mails
Common Features of E-mail Phishing

• Too good to be true
  • Nigerian prince inheritance scam no longer works
  • But free offers from Amazon do succeed

• Sense of Urgency
  • Act now

• Hyperlinks – slight modification
  • www.bankofarnerica.com - the 'm' is actually an 'r' and an 'n'

• Attachments
  • Don’t open unless you are expecting one

• Unusual sender
Consequences of a Successful Phish

• Unintended Consequences
  • Financial loss – payroll change of accounts
  • Clicking on a miscellaneous web link
    • Disclosure of personal information
    • Infecting computer and network
    • Disclosure of e-mail password
      • A disaster -- as e-mail access linked to resets of many systems including banking
      • 2017 Verizon Data Breech Digest found 90% of data loss incidents had its root in successful phishing
What can be done?

• Controls in place to verify changes requested from e-mail
• Provide staff with example of phishing e-mails
• Consider a commercial testing/training resource
  • Wayne RESA – 2nd year with KnowBe4
    • Provides simulated phishing e-mails and training resources
    • Helps staff recognize telltale signs of malicious e-mails
      • Wayne RESA not “keeping names” – when links are “clicked”
    • Staff proud that they can recognize harmful e-mails
      • They need to be complimented
  • Lots of free resources: https://www.knowbe4.com/
    • Approximately $8 per year per employee
    • Product overview: https://www.knowbe4.com/hubfs/KnowBe4-Presentation-Overview.pdf
From: MIR Giveaway <Giveaway@MIRTheatres1219.com>
Sent:
To: user@example.com
Subject: MIR Star Wars Giveaway - 10,000 Free Tickets

To celebrate MIR Theater's 35th anniversary, we are giving away 10,000 tickets to see Star Wars: The Last Jedi.
The promotion ends at 9:00PM EST on Dec 15th. All you have to do is head over to our website and pick a city and a time you want to see the movie. It will then supply you with a code that you can redeem at any MIR Theater for the movie ticket. The tickets will be given away on December 15 at 10:00 PM.

Enter the giveaway

Mike Mihalich, MIR Digital Cinemas
Phishing Exercises Get Staff Thinking

- Comment from a RESA Staff member

**Subject:** RE: Report on MJR Star Wars Giveaway - 10,000 Free Tickets e-mail

Hi Jim,

I **KNEW** it! I stayed away from it, although it did look enticing. My compliments to you and/or whoever else on your staff is coming up with these emails. They’re really authentic. I Googled the name at the end of the email (Mike M), and of course he’s the founder/CEO of MJR Theatres. That REALLY made it seem authentic!

I didn’t have time yesterday, but I’m so overly-suspicious of these types of emails, if I really wanted to see if there was a ticket giveaway, instead of clicking the link, I would have just found the official MJR website to see if anything was there. (I wasn’t always like that, but I seem to be suspicious of everything now—maybe TOO suspicious.) I’m sure I am not the only one who would have tried another way to check; just thought I’d share my thoughts with you.

Thanks and have a great weekend,
How Are We Doing?

- Free Movie Tickets
- More challenging tests

**Overview**

- **224** Recipients
- **100%** Delivered
- **21%** Opened
- **7.1%** Clicked

**Industry Benchmark Data**

- **YOUR LAST PHISH-PRONE%**: 33.2%
- **INDUSTRY PHISH-PRONE%**: 31.4%

Industry: Education
Technical Resources

• Tighten spam filter rules – more e-mail to junk or discard

• Microsoft Office 365 users
  • Consider higher levels of license A3 or A5
  • Participate in new statewide Office 365 admin group
    • Contact Nicholas Hay, Monroe ISD, Nicholas.Hay@monroeisd.us

• KnowBe4 MSBO discount offer
  • See presentation materials folder
At Oakland Schools..

Security is not a destination it is a journey.
Part of the Journey

Biweekly Security Team Meetings

• Review new threats
• Review cyber events past two weeks
• Project based security updates
Passwords

They are not a security tool any longer.

Review all applications for authentication methods
Two-Factor Authentication

Two factor strengthens access security by requiring two methods to verify your identity. Something you know, plus something you have.
Roll out - Summary

- Oakland would do this again in a heartbeat
- Implement on leadership first
- Use a phased-in approach
- People will be angrier than you think
- You can’t over communicate
DUO Platform
SIEM

Security information and Event Management
<table>
<thead>
<tr>
<th>Bidder Name</th>
<th>Notarized Family Relationship Disclosure Form</th>
<th>Certification Form</th>
<th>Equal Opportunity Policy Form</th>
<th>Acknowledged 1.3</th>
<th>Addendum</th>
<th>Completed</th>
<th>WE</th>
<th>Security Monitoring Services All Hours Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creative Breakthroughs, Inc.</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>y</td>
<td>$186,580.00</td>
<td></td>
</tr>
<tr>
<td>CDW Government LLC</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>y</td>
<td>$187,500.00</td>
<td></td>
</tr>
<tr>
<td>Navicaste, Inc</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>y</td>
<td>$198,000.00</td>
<td></td>
</tr>
<tr>
<td>Securely Yours, LLC</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>y</td>
<td>$86,400.00</td>
<td></td>
</tr>
</tbody>
</table>
Protect

Tools we use to protect students and district data

- Firewalls
- Antivirus
- Patching
- Filtering
- Training
Detect

System alerts

Behavioral based notifications - High Bandwidth, CPU

New version notifications
Detect

Dashboard

Alarm
### Response

- Escalation
- Prioritization
- Mitigation

<table>
<thead>
<tr>
<th>LAST SEEN</th>
<th>VULNERABILITY ID</th>
<th>VULNERABILITY NAME</th>
<th>LABELS</th>
<th>SEVERITY</th>
<th>SCORE</th>
<th>FIRST SEEN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mon, Sep 17, 2018, 10:38 AM EDT</td>
<td>CVE-2018-3646</td>
<td>Microsoft Guidance to mitigate LITF variant - ADV...</td>
<td></td>
<td>Medium</td>
<td>4.7</td>
<td>Mon, Sep 17, 2018, 10:3...</td>
</tr>
<tr>
<td>Mon, Sep 17, 2018, 10:38 AM EDT</td>
<td>CVE-2018-3615</td>
<td>Microsoft Guidance to mitigate LITF variant - ADV...</td>
<td></td>
<td>Medium</td>
<td>5.4</td>
<td>Mon, Sep 17, 2018, 10:3...</td>
</tr>
<tr>
<td>Mon, Sep 17, 2018, 10:38 AM EDT</td>
<td>CVE-2018-3620</td>
<td>Microsoft Guidance to mitigate LITF variant - ADV...</td>
<td></td>
<td>Medium</td>
<td>4.7</td>
<td>Mon, Sep 17, 2018, 10:3...</td>
</tr>
<tr>
<td>Mon, Sep 17, 2018, 10:38 AM EDT</td>
<td>CVE-2017-5754</td>
<td>Rogue data cache load vulnerability - CVE-2017-5...</td>
<td></td>
<td>Medium</td>
<td>4.7</td>
<td>Mon, Sep 17, 2018, 10:3...</td>
</tr>
<tr>
<td>Mon, Sep 17, 2018, 10:38 AM EDT</td>
<td>CVE-2017-5715</td>
<td>Branch target injection vulnerability - CVE-2017-5...</td>
<td></td>
<td>Medium</td>
<td>4.7</td>
<td>Mon, Sep 17, 2018, 10:3...</td>
</tr>
</tbody>
</table>
Recovery

- Backup - Where are they? How fast to recover?
- Failover
- Restore
- Prevention - Generators, Network Redundancy and Testing
Questions