PARAGON DEVELOPMENT SYSTEMS

3.05.2019

Agenda

Planning For and Responding To Cyber Attacks

1. Introduction to PDS and WRPS
2. Why Pen Test?
3. What Are The Threats?
4. School District Experience
5. Best Practices
6. Resources

Wisconsin Rapids Public Schools Profile

- North Central Wisconsin
- 5100 Students
- 700 Staff
- 12 Buildings

PROFESSIONAL SERVICES

Solutions Aligned With Your Goals

The Power of PDS

PDS delivers devices, solutions, and services that put your focus on improving student outcomes and providing end users an outstanding technology experience.

PDS invests in smart, qualified experts that help you solve technology problems.

Digital Infrastructure

Solutions:

- Data Center Storage & Backup
- Virtualization
- Network Architecture
- Network Access Control
- Firewall Unified Threat Management

Why Pen Test?

The Goal of Penetration Testing

- Accurately Emulate An Actual Attack
- Identify Vulnerabilities And Risks
  - Confidentiality—Who has access to data?
  - Integrity—Accuracy of data
  - Availability—Ransomware
- Provide Steps For Remediation
- Encourage Contingency Planning

CYBERSECURITY ISSUES FOR K12

EXTERNAL THREATS

- ACH banking fraud
  - Accounts payable being conned into paying false accounts
- Hackers
  - Chinese and Russian threats are especially persisting for malware, ransomware and phishing
  - Financial and student database apps are prime targets for a quick sell on the dark web
- W2 fraud
  - Stolen faculty/staff PII, file false tax returns

INTERNAL THREATS

- Bad leavers
  - Staff that are fired or resign and cause problems as they leave
- Poor endpoint security
  - Access controls, anti-virus management, encryption
- Poor network segmentation
  - Allows Malware/Ransomware to quickly gain a foothold and spread
- Users (Faculty/Staff/Students)
  - Malicious or rogue users
  - Careless users

Why Did We Consider Testing?

- Completed District Security Assessment
  - Available from CoSN - http://cosn.org/download-cybersecurity-self-assessment
- Numerous changes to network infrastructure
- New firewall
- Continuous threat risk
- Recommendation from:
  - Insurance carrier
  - Financial Institution (specifically in relation to payroll transactions)
- Recent Breaches

How did we gain support and approval from Admin and School Board?

- Explained risks and threat potential
- Explained the cost of mitigation if a breach was encountered
- How do you know you have a good defense without someone trying to get in?
  - Need to test our firewall
  - Need to identify vulnerabilities
  - We don’t know what we don’t know

What was the testing process like?

- Initial discussion with Sikich/PDS
  - Discuss environment
  - Discuss outcomes WRPS was expecting
  - Determine what to services to and systems to test
- Run initial scans
  - Identified a few servers open to public that shouldn’t have been (HVAC!)
  - Determine what IP’s to test (internal and external)
- Run Testing
  - Most testing occurred after 3pm
  - Tested for several days

What was the testing process like? (Cont'd)

- Discuss Results
- Remediate problem areas
  - Sikich did a great job of identifying how to fix problem areas
- Re-test
- Discuss Outcomes/Close out initial testing
- Scan every 3 months for first year

What did we test?

- Internal and external penetration test
  - Servers
  - Attempt to Breach Firewall (open ports)
  - Internal – Plugging into network inside
  - Desktop – Teacher Workstation
- Web Applications
  - Alio – Financial System (internal only)
  - Employee Service Portal
  - Skyward
- Mobile Apps
  - Skyward
  - Alio – Employee Service Portal
- We did not engage in any social engineering tests

What did the test results yield?

- 8 High Risks, 7 Medium Risks, 0 Low Risks
- External Testing
  - Potential sensitive information (School Board Meeting Minutes)
  - Exposed one instance of TFTP (Trivial File Transfer Protocol)
- Web Application Testing
  - Identified one Skyward vulnerability
    - Contacted Skyward to remedy
  - Alio Financial Software
    - Many vulnerabilities identified
    - Contacted Alio to remedy

What did the test results yield?

- Internal Testing
  - Stole encrypted user credentials, then cracked multiple sets of teacher credentials
  - Located local admin passwords on Windows machines
  - Gained remote access to multiple systems and compromised multiple user credentials
  - Identified several machines that were vulnerable to high-profile remote-code execution bugs
  - Sikich was unable to gain domain administrative privileges
- Remediation
  - Sikich identified ways to minimize vulnerabilities
  - After remediation recommendations
    - 5 high risk, 3 medium, 0 low
    - 4 risks were with software we purchased (Skyward and Alio)
    - Others were items were in process of remediation at time of re-test
    - Weak Password Policy

pds

Key Takeaways/Changes

- Hard to know what is vulnerable without testing
- Discovered unsecured server open to the public
- Needed to cleanup internal policies on Windows
- Patch and update Servers regularly
- Installed dedicated payroll computer
- Outside of network - relatively secure
- Inside of Network - needed to do some cleanup

HARDEN YOUR ENVIRONMENT AND PEOPLE

SECURE YOUR ENVIRONMENT

- Evaluate your **firewall rules** regularly.
- Implement **network segmentation**. Flat networks are easy targets.
- Implement **two-factor authentication** on critical infrastructure
- Have strong **password requirements**.
- Have strong **spam filtering**.
- Limit **administrative rights** on workstations to those users whom absolutely need it.
- Limit or securely implement **remote access**.
- **Patch**, patch, patch..
- Perform an annual **risk assessment** of the threats and vulnerabilities facing your district.
- Perform ongoing **vulnerability scans** and annual **penetration testing**.

SECURE THE PEOPLE

- Have a robust **information security policy** and enforce it.
- Have an **incident response plan** and test it.
- Have a **security awareness training program** and make it a part of your onboarding and periodic trainings.
- **Phish** your own users, raise awareness why security is important.
    - Financial impacts from lawsuits, fines or penalties
    - Legal impacts as a result of non-compliance with contractual obligations, laws, or regulations
    - Reputational impacts

Incident Response Resources

- https://wetlcosn.org/cyber-security/
- Center for Internet Security
  - https://www.cisecurity.org/
  - https://www.cisecurity.org/isac/
- **Notify Your Most Trusted Technology Partner**
  - **PDS 1-877-737-7211**
- +1 (866) 923-0907 and/or **emergency-response@checkpoint.com**
- **Insurance Provider**

Incident Response (cont.)

- US Dept. of Education
  - https://studentprivacy.ed.gov/resources/data-breach-response-checklist
  - https://studentprivacy.ed.gov/resources/data-breach-response-training-kit

Next Steps

- If you would like to understand the costs of testing for your district please contact me at: dblakeslee@pdsit.net or 608-213-7880.

- We can generate a proposal that fits your budget after one 30-40 minute phone call.

Questions?

Visit PDSIT.net for more information!

Thank You

Derek Blakeslee
dblakeslee@pdsit.net
[608] 213-7880

PDSIT.net