The K-12 Overlooked Critical Technology Infrastructure

NYSAIS Business Affairs Conference 2018

03/06/2018
Summary

- What are the emerging cyber threats to schools?
- Who is targeting schools?
- Why are schools being targeted?
- How are schools being targeted?
- What can schools do to protect themselves?
The Headlines
Each threat actor has different motivations, capabilities, and resources.
Current Cast of Actors

What do they want?

- Money (Ransomware)
- Personal Information (PII/PHI)
- Credentials
- Proprietary Information
- Resources (CPU/Storage/Botnets)

Source: [https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/](https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/)
What is the Motivation?

76% of breaches in 2017 were financially motivated

**Source:** Verizon 2018 Data Breach Investigations Report, 11th edition
How do they get in?

Exploit a vulnerability

- Misconfiguration
- Technical Flaw
- Design Flaw

We let them in

- Social Engineering
Anatomy of an Attack

Threats to Schools

- Denial of Service
- Ransomware
- Social Engineering
FBI Notification: January 31 2018

As of January 2018

- 69 Intrusions
- Attempted sale of 100 million records
- Release of 200,000 records
- PII of 7000 students

Source: https://www.databreaches.net/fbi-private-industry-notification-warns-schools-about-thedarkoverlord/
Don’t believe me? Ask the FBI

Denial of Service

- Deny legitimate users access to a service
- Denial of Service vs Distributed Denial of Service
- Exploit Vulnerability
- Volumetric, Protocol, Application
Mitigating DoS and DDoS

- Work with your Internet Service Providers (ISPs)
- Third party DDoS protection service
- Patch Systems
- Multiple WAN entry points
Ransomware

- Malware
- Several Delivery Methods
- Extortion
- Business Case
- Cryptocurrency
Oh Ransomware, How Popular Are We!

- Opportunistic and Targeted
- Little Risk or Cost
- Monetizing stolen data not required
- Can infect a large number of devices across a network

Mitigating Ransomware

- Backup, Backup, Backup! (3,2,1 rule)
- Security Awareness Training
- Patch, patch, patch!
- Malware Detection/Prevention
- Secure Configurations
Social Engineering?

- Phishing*
- Spearphishing*
- Whaling
- Vishing
- SMiShing
Success of Spearphishing

2016
• 7.3% Total Click rate
• 15% Fooled Twice
• 3% Fooled Thrice
• 1% Hopeless

2017

Phishing and pretexting represent 98% of social incidents and 93% of breaches. Email continues to be the most common vector (96%).
Psychology of Social Engineering

- Fear
- Obedience
- Greed
- Helpfulness
Patch the Human!

- Follow established business rules
- Listen to your instincts, if it doesn’t feel right then most likely it isn’t
- Look for irregularities
- If you click it, Report it!

Human v2.1.1
Why Schools?

- Low-Hanging Fruit
- Large Collection of PII/PHI
Why Schools?

- Budget
- Staffing
  - Who is responsible for security?
- Challenging Environment
  - Open and Collaborative Environment
  - Technology Enabled/Dependent
Impact to Schools

- Financial Impact
- Operational Impact
- Regulatory/Litigation
- Hidden Costs
What can we do?

- Appropriate Use Policies
- Authentication
- Segmentation
- Secure Configuration Baselines
- Risk-based, Holistic and Layered
## Critical Security Control (Industry Standards)

<table>
<thead>
<tr>
<th>Critical Security Control</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory of Authorized and Unauthorized Devices</td>
<td>Medium</td>
</tr>
<tr>
<td>CSC 2 Inventory of Authorized and Unauthorized Software</td>
<td>Low</td>
</tr>
<tr>
<td>Secure Configurations for software and hardware</td>
<td>Medium</td>
</tr>
<tr>
<td>Continuous Vulnerability Assessments and Remediation</td>
<td>Medium</td>
</tr>
<tr>
<td>Controlled use of administrative privileges</td>
<td>Low</td>
</tr>
<tr>
<td>Maintenance monitoring and analysis of audit logs</td>
<td>High</td>
</tr>
<tr>
<td>Email and Web browser Protections</td>
<td>High</td>
</tr>
<tr>
<td>Malware Defenses</td>
<td>Medium</td>
</tr>
<tr>
<td>Limitation and Control of Network Ports</td>
<td>Low</td>
</tr>
<tr>
<td>Data Recovery Capability</td>
<td>High</td>
</tr>
<tr>
<td>Secure Configuration of Network Devices</td>
<td>Medium</td>
</tr>
<tr>
<td>Boundary Defense</td>
<td>Medium</td>
</tr>
<tr>
<td>Data Protection</td>
<td>Medium</td>
</tr>
<tr>
<td>Controlled access based on need to know</td>
<td>Low</td>
</tr>
<tr>
<td>Wireless Access Control</td>
<td>Medium</td>
</tr>
<tr>
<td>Account Monitoring and Control</td>
<td>Medium</td>
</tr>
<tr>
<td>Security Skills Assessment and Appropriate Training to Fill Gaps</td>
<td>Medium</td>
</tr>
<tr>
<td>Application Software Security</td>
<td>Medium</td>
</tr>
<tr>
<td>Incident Response and Management</td>
<td>High</td>
</tr>
<tr>
<td>Penetration Tests and Red Team Exercises</td>
<td>Low</td>
</tr>
</tbody>
</table>
Helpful Sites

- National Institute of Standards and Technology (NIST) Cybersecurity Framework: [https://www.nist.gov/cyberframework](https://www.nist.gov/cyberframework)
- K-12 Cyber Incident Map: [https://k12cybersecure.com/map/](https://k12cybersecure.com/map/)
- FBI Safe Online Surfing Program: [https://sos.fbi.gov/](https://sos.fbi.gov/)
Questions?

Jacob (Jake) Lehmann
Email: jlehmann@friedmancyzen.com

William (Will) Mendez
Email: wmendez@friedmancyzen.com
Backup Slides
What do they want?

HACKED PC

- Phishing Site
- Malware Download Site
- Warez/Piracy Server
- Child Pornography Server
- Spam Site

- Webmail Spam
- Stranded Abroad Advance Scams
- Harvesting E-mail Contacts
- Harvesting Associated Accounts
- Access to Corporate E-mail

- Online Gaming Characters
- Online Gaming Goods/Currency
- PC Game License Keys
- Operating System License Key

- Facebook
- Twitter
- LinkedIn
- Google+

- Web Server

- Bot Activity
- Spam Zombie
  - DDoS Extortion Zombie
  - Click Fraud Zombie
  - Anonymization Proxy
  - CAPTCHA Solving Zombie

- Virtual Goods

- Account Credentials
  - Online Gaming Credentials
  - Web Site FTP Credentials
  - Skype/VOIP Credentials
  - Client Side Encryption Certificates

- Financial Credentials
  - Bank Account Data
    - Credit Card Data
    - Stock Trading Account
    - Mutual Fund/401k Account

- E-Mail Attacks

- Hijacking
- Reputation Hijacking

- Hostage Attacks

- Fake Antivirus
  - Ransomware
  - Email Account Ransom
  - Webcam Image Extortion
Breaches expose 50,000 student and teacher records at Leon County Schools; more districts likely affected

The records of roughly 50,000 students, parents, teachers and staff members from the Leon County Schools (LCS) District in Tallahassee, Fla. were compromised in two related breach incidents involving a third-party education services provider.

But district superintendent Rocky Hanna warns that this is likely just the tip of the iceberg, stating in a press conference that more than 368,000 records were actually found exposed -- meaning several other schools across Florida are presumably also affected.
What have they gotten?
Identifying Spearphishing

IT HELP DESK

To:

Hello,

In an effort to continue bringing you the best available technology, our team has implemented the newest version of Microsoft’s Office 365 Webmail. Your existing emails, contacts, and calendar events will be seamlessly transferred to your new account.

Visit MailScanner has detected a possible fraud attempt from "mail....com" claiming to be https://login.microsoftonline.com and login with your current username and password to confirm your new account.

Kind Regards,

Director of Information Technology
Ph: (855) 999-999
Fax: (855) 999-999

This email and the attachments may contain information that is privileged or confidential, which may include protected health information that is subject to protection under federal and state laws, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This email and its attachments are intended solely for the use of and the individual or entity to whom it is addressed. If you are not the intended recipient, you are hereby notified that any review, dissemination, distribution, printing, copying or other use of this email message and/or any of its attachments is strictly prohibited, and may subject you to criminal or civil penalties. If you have received this transmission in error, please immediately notify the Compliance Officer at telephone (877) 999-999 and permanently delete this email as well as its attachments.

Please DO NOT REPLY to this email as this is not a monitored inbox. If you have questions/inquiries please visit MailScanner has detected definite fraud in the website at "www.google.com". Do not trust this website; https://ithelpdesk....com.