DOE Technology and Security Updates

2016 FAMIS Conference

Presenters:
Gary Evans, Ted Duncan

Tallahassee, FL
June 21 – 23, 2016

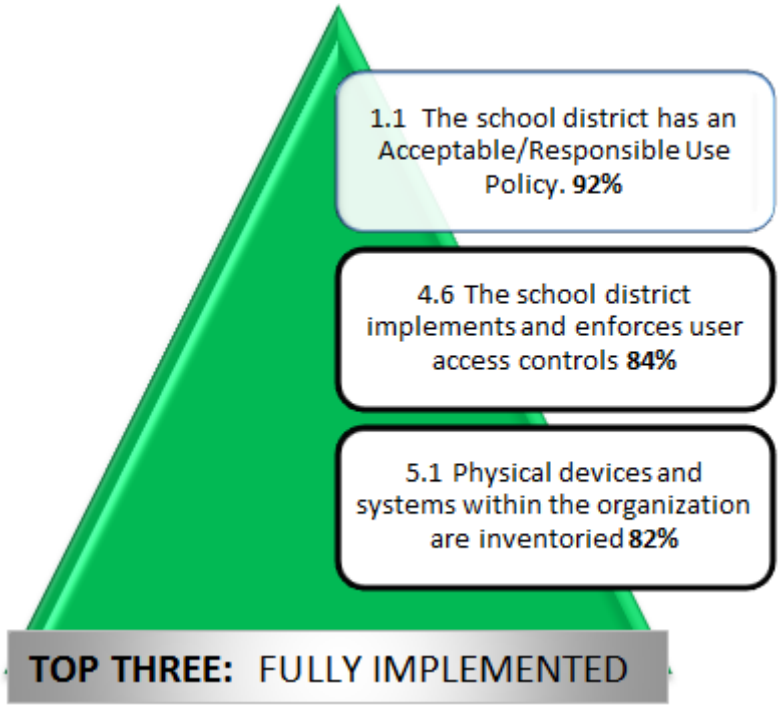
FLORIDA DEPARTMENT OF EDUCATION
fldoe.org

FLORIDA DEPARTMENT OF EDUCATION
fldoe.org

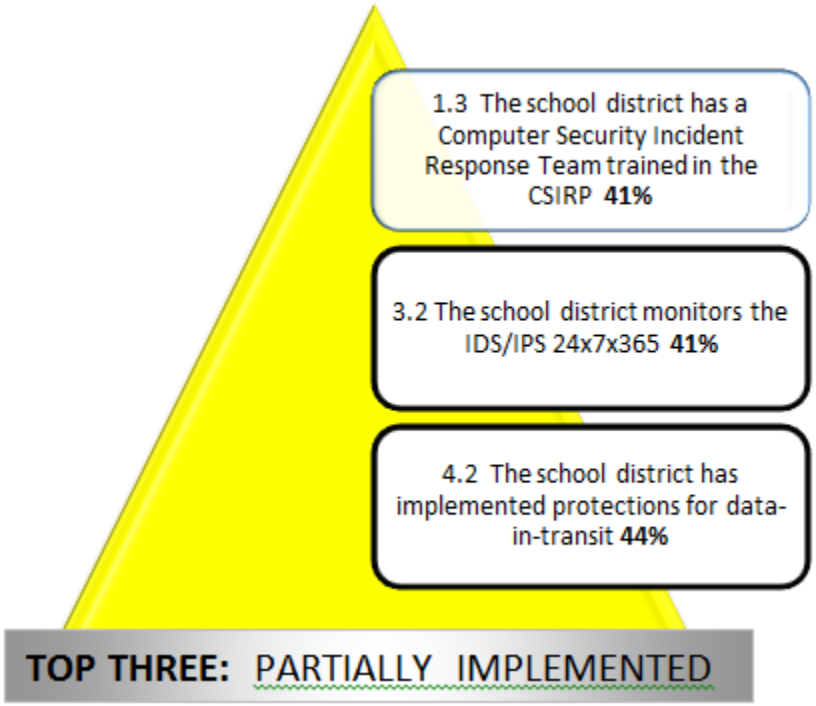
Purpose

- Review progress by Districts of Security Best Practices.
- Spring 2016 Activities
- Discuss Superintendent's Security Questionnaire
- Focus on DDoS

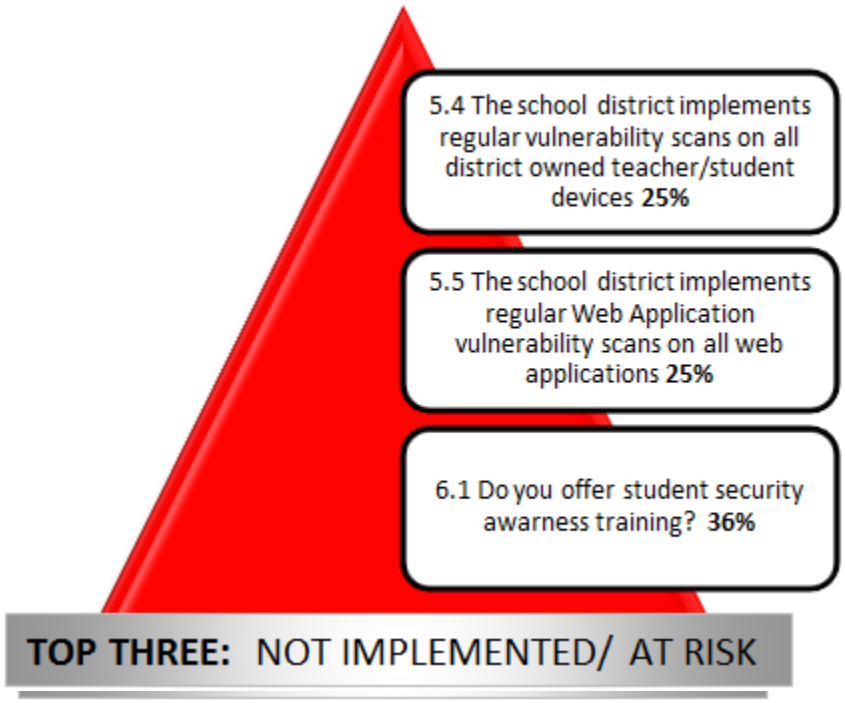
Implementation: Top Three District Reported Fully Implemented



Implementation: Top Three District Reported Partially Implemented



Implementation: Top Three District Reported Limitedly Implemented



Governor's Executive Order #2013-276 Florida Plan for Education Accountability

- Section 2. Student Data Security of Executive Order
  - (a) The Commissioner of Education shall immediately conduct a student data security review and issue policies, including internal protocols and operating procedures, for the Department, school districts, and any assessment provider or other entity with access to student data, in order to protect student information and prevent any unintended use or release of such information.
  - (b) The Commissioner of Education shall also make recommendations regarding any needed rule or legislative change to safeguard the privacy of our students' data by December 31,2013.
  - (c) The Commissioner of Education shall ensure that adequate protections are in place to ensure that no agency, public school, center, institution, or any other entity that is part of Florida's education system releases a student's education records without the written consent of the student or parent to any individual, agency, or organization, except as specifically provided by Florida law.

- Commissioner's Report:
  - Report provided direction to Agency and Districts on steps to improve Student Data Security
    - Report online at http://www.fldoe.org/core/fileparse.php/5390/urlt/0081020-datasecurityreport.pdf
  - Report list areas for Improvement and places emphasis on Best Practices

Spring 2016 Activities

- FDOE worked with AIR and Pearson before Spring statewide assessments to make sure a response plan for security threats was in place.
  - Centralized testing systems are the hub of the testing services, but districts are the spokes in the testing process.

- FDOE implementation of strong DDoS mitigation services

- March Superintendent's questionnaire was distributed by Commissioner to ensure best practices for security and mitigation was in place at school districts.
  - 11 Questions on Best Practices

Superintendent's Security Questionnaire

- Commissioner's March communication to Superintendents ahead of Spring Assessments to ensure security Best Practices are in place to mitigate interruption in assessments.

  - Have you established with your Internet Service Provider (ISP) edge protection?
  - Do you have mitigation plan with your ISP provider?
  - Have you patched applications and operating systems with updates?
  - Have you hardened (turned off unnecessary services and changed default passwords) your network devices and servers?
  - Are you running vulnerability scans?
  - Anti-malware is current and running?
  - Are you limiting administrative access to network, servers, and applications?
  - Are you monitoring all network traffic and have set baseline performance metrics?
  - Do you have security incident response plan?
  - Do you have plans to participate in the infrastructure trials for testing?
  - Have you taken steps to ensure that networking equipment, including routers and wireless access points, can handle the connections required for the students testing concurrently in a single location?

Has infrastructure been stress tested?

- Ahead of large-scale testing, have pilots been run with a representative sample of students at a location.
- Ensures that network capacity and access points can handle testing traffic.
- Can be a challenge, understanding that this takes away valuable classroom and/or staff time.
- Infrastructure trials for statewide testing help establish readiness.

Questionnaire Reference: Have you taken steps to ensure that networking equipment, including routers and wireless access points, can handle the connections required for the students testing concurrently in a single location? Do you have plans to participate in the infrastructure trials for testing?

Is server and device hardening part of the build and deployment process?

- Shutting down unnecessary services or network ports.
- Changing default server and device accounts.
- Documenting hardening as part of the build and deployment checklist.
- Hardening establishes a baseline build.

Further reading: https://www.sans.org/reading-room/whitepapers/bestprac/practical-methodology-implementing-patch-management-process-1206

Questionnaire Reference: Have you hardened (turned off unnecessary services and changed default passwords) your network devices and servers?

Are servers and software being patched for latest vulnerabilities?

- Are there established procedures for implementing in test and production environments?
- Is there a plan for installing and for backing out?
- Most districts have this in place, with almost all planning to have this implemented by the end of summer

Further reading: https://www.sans.org/reading-room/whitepapers/bestprac/practical-methodology-implementing-patch-management-process-1206

Questionnaire Reference: Have you patched applications and operating systems with updates?

Are vulnerability scans being run?

- Check Gartner for analysis of tools
  - https://www.gartner.com/doc/reprints?id=1-2KU6P9E&ct=150807
- Can be done by cloud providers.
- Most districts are scanning or are implementing scanning by the end of the summer.

Is anti-malware current and running?

- Check Gartner for analysis of tools for endpoint protection:
  - https://www.gartner.com/doc/reprints?id=1-2XU816T&ct=160203
- Some ISPs offer anti-malware scanning as a service.
  - FIRN/MFN offer these services.
- Almost all districts are on-target to have a solution in place by the end of summer.

FIRN Offering Secure Bundled Internet Security Services:
http://www.dms.myflorida.com/business_operations/telecommunications/suncom2/data_services/florida_information_resource_network_firn/firn_security_services

Questionnaire Reference: Anti-malware is current and running?

Is admin access restricted?

- Is access restricted on servers, network devices, shares and applications?
- Is an audit process in place to check access?
- Every district has implemented some form of access restrictions.

Is network traffic being monitored?

- Is IDS and IPS implemented?
  - IDS and IPS can be provided by third parties
  - FIRN/MFN offers these services through FIRN Secure Bundled Internet Security Services

- Have baselines for normal traffic been established?
  - Unexpected changes to inbound or outbound bandwidth can be an attack symptom

FIRN Secure Bundled Internet Security Services:
http://www.dms.myflorida.com/business_operations/telecommunications/suncom2/data_services/florida_information_resource_network_firn/firn_security_services

Questionnaire Reference: Are you monitoring all network traffic and have set baseline performance metrics?

Attack Mitigation Plans

- Local incident response plans.
  - Is a plan in place for communication with district staff, schools, parents?
  - Do you have contacts with local law enforcement, FDLE and FBI?

- Incident response plan with ISP?
  - Is an SLA in place with your ISP that deals specifically with DDoS attacks?
  - Is your ISP monitoring and taking steps on your behalf when DDoS is detected?
  - Do you have a single point of contact (dedicated customer service representative) that can escalate issues quickly?
  - How are detected attacks and mitigation communicated to you?

Questionnaire Reference: Do you have security incident response plan? Do you have mitigation plan with your ISP provider?

Has Edge Protection From DDoS Been Established?

- Rise in the number of incidents reported during FSA testing.
- Barriers to entry are much lower to perform DoS/DDoS.
- Different reasons for DDoS attacks
  - Political agenda
  - Student driven

Questionnaire Reference: Have you established with your Internet Service Provider (ISP) edge protection?

Has Edge Protection From DDoS Been Established?

- Edge protections and mitigation aren't new, but are being more widely used as attacks become more prevalent.

- Mitigation services and WAF protect against threats before they reach your data circuit.
  - Protect against volumetric attacks
  - Protect against slow attacks that consume resources
  - Protect against include or injection attacks
  - Discard unwanted traffic before it reaches your data circuit (ex. UDP, used in volumetric attacks)

Questionnaire Reference: Have you established with your Internet Service Provider (ISP) edge protection?

Edge Protection and Mitigation Offerings

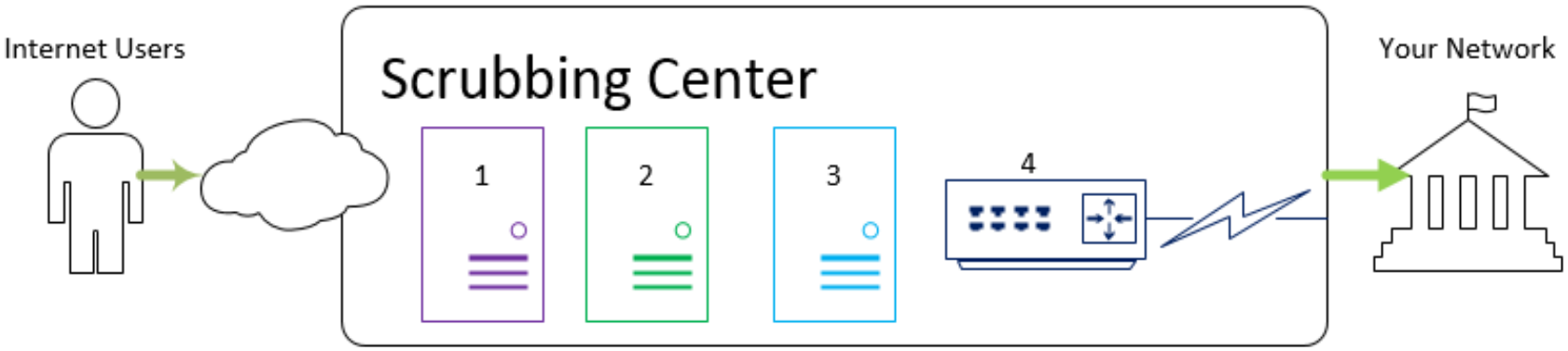
- Most ISPs in Florida provide some level of DDoS mitigation services, most often at a premium.
- A number of third-party cloud providers are available, with ranges of service levels and costs.
- Important to find the right blend of services for budget.
- Some providers include value added services, like application management, client reputation scoring and CDN for districts that host applications.

Questions to Ask Mitigation Providers

- How much clean bandwidth will your provider guarantee?
- Incident response time?
- Dedicated customer service representative?
- Who answers the phone? Tier 1 call center or an engineer?
- Is the service “always on” or “always available”?
- How many scrubbing centers are available and where are they?
- What has been their experience with mitigation? Largest volumetric attack mitigated? Most challenging mitigation?
- Is there a staging environment for policy changes?
- What value added services are offered?
- What is the onboarding process?
  - How soon do you need it?
- What is the process for leaving the service?
- What reporting services and logging are available?
  - Including baselines and services under stress.

Scrubbing Center 101

Vendors do things differently, but achieve the same outcomes.



1. Gathers traffic data for analysis
2. Null-routes bad traffic based on known threats or ACLs
3. Removes transport and application layer attacks
4. Encapsulates clean traffic over a GRE or proxy tunnel to client network

FDOE's Implementation Overview

- Mitigation is not "one size fits all"
- FDOE has mitigation services hosted at NWRDC and through DDoS service providers
- FDOE is selecting a permanent solution for 16/17

FDOE's Implementation

- Protecting servers at NWRDC

- Using third-party platform provider
  - "Always On" Mitigation
  - WAF
  - Using client risk scoring to deny access to bad actors
    - Bad actors can include clients using known attack vectors or potentially detrimental activity, like screen scraping.
  - Also using vendor's integrated CDN
    - 75% of traffic is served from the edge cache.
    - Tuning activity is peaks at the beginning with a steep decline once stable.
  - Routing data to scrubbing centers using DNS with future plans to use BGP routing for our public addresses.

Discussion

Links to Resources

Gartner – Magic Quadrant for Endpoint Protection Platforms
https://www.gartner.com/doc/reprints?id=1-2XU816T&ct=160203
Gartner - Magic Quadrant for Application Security Testing
https://www.gartner.com/doc/reprints?id=1-2KU6P9E&ct=150807
SANS Institute - A Practical Methodology for Implementing a Patch Management Process
https://www.sans.org/reading-room/whitepapers/bestprac/practical-methodology-implementing-patch-management-process-1206
FIRN Secure Bundled Internet Security Services Features And Pricing:
http://www.dms.myflorida.com/business_operations/telecommunications/suncom2/data_services/florida_information_resource_network_firn/firn_security_services
FIRN / Palo Alto Networks Next Generation Firewall Features:
https://paloaltonetworks.com/products/features/application-visibility.html

FLORIDA DEPARTMENT OF EDUCATION
fldoe.org

Contact Information

OTIS

Email: gary.evans@fldoe.org

ted.duncan@fldoe.org

Phone: (850) 245-9691

(850) 245-9828

www.FLDOE.org