State Cyber Incident
IT Q&A CALL

August 2, 2019, 10:30 AM

Agenda

- General Updates on Status
- Reporting an Incident
- Action Steps for School Systems
- Phased Process and Q&A

Status Updates

- Current status of districts, charters and non-publics
- We can not iterate enough, about the importance of this process.

Reporting an Incident

If your school identifies a cyber incident/cyberattack on your campus:

1. Report the incident to the Louisiana Department of Education at EdTech@la.gov and/or call Carol Mosley at 225-588-5584
2. Contact your Parish's OEP Director. The OEP Director will be in charge of filing the necessary paperwork for engaging any necessary state resources including but not limited to the Governor's Office of Homeland Security, Office of Technology Services, National Guard, and Louisiana State Police.

Action Steps for School Systems

- Complete the Critical Task List for School Systems. Phase 1 should be completed immediately.
- Complete the LDOE Cyber-security Follow-up Status Survey – CONTINUE TO UPDATE UNTIL YOU HAVE COMPLETED ALL OF THE PHASES

UPDATES

IOCs Identified:

- Continuous connections through LogMeIn
- Web base logins through Advapi
- Presence of advapi32.dll from trampolined processes
- Unauthorized users created with elevated privileges
- Outbound web traffic to ports 445/447/449/8082/16993
- Traffic to or from Pastebin.com (104.20.209.21) in the previous two weeks
- Attempted connections to .onion sites
- Presence of tiki.exe in startup programs
- Unauthorized presence or use Ccleaner.exe0
- Presence of tiki.exe, id_up.exe or wdcsam.inf.2823sf8551
- Connections to: 84.146.54.187, 75.147.173.236, 218.16.120.253, 170.238.117.187, 195.123.237.129, 194.5.250.123, 85.204.116.158, 31.184.254.18 or 186.10.243.70
- Hashes to watch for:
  - MD5 d41d8cd98f00b204e9800998ecf8427e
  - SHA1 da39a3ee5e6b4b0d3255bfef95601890afd80709
  - SHA256 e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

Phased Process and Q&A

Emergency Cyber Incident Prevention Critical Task List - Phase 1

- Turn off all internet access in all locations.
  - Primary site.
  - All schools (including any private DSL lines).
  - All other ancillary sites.
  - WAN circuits can remain connected for inter-office connectivity. This is only targeted at locations where internet access exits or enters the network.
- Once all above actions in Phase One have been completed and verified, proceed to Phase Two.

Phased Process and Q&A

Emergency Cyber Incident Prevention Critical Task List – Phase 2

- Begin allowing the following critical services out the network in this specific order:
  - Allow DNS servers to communicate over port 53 (TCP and UDP) outbound to known external DNS servers ONLY. Do not allow to all destination IP addresses.
  - Allow email servers to communicate outbound to required destinations ONLY.
    - If Microsoft O365 is used, only allow email servers to identified Microsoft address ranges (included in the critical task list)
    - If Google Email is used, only allow email servers to identified Google address ranges. (included in the critical task list)
    - If you have an onsite Exchange environment, only allow SMTP TCP port 25 and 587 to and from your external mail gateways.
    - For all other email services, contact your vendor for assistance.
- Allow connections necessary for SIS, payroll and finance systems to function normally. This should only be allowed by explicit source IPs, destination IPs, and destination ports. This should only be allowed by explicit source IPs, destination IPs, and destination ports.
- Allow all connections necessary for phone systems to function.
- The following external State of Louisiana IP ranges can be safely allowed:
  - 204.196.0.0/16
  - 159.39.0.0/16
  - 170.145.0.0/16

  NOTE: At this point, connectivity to internal resources should still be working.
- Once all above actions in Phase Two have been completed and services verified by business owner, reboot all Windows workstations and servers then proceed to Phase Three

Phased Process and Q&A

Emergency Cyber Incident Prevention Critical Task List – Phase 3

- Allow connections necessary for payroll, finance, and human capital management systems to
- function normally. This should only be allowed by explicit source IPs, destination IPs, and
- destination ports.
- Allow connections necessary for student systems (e.g. SIS, health, food service, transportation
- and safety systems) to function. This should only be allowed by explicit source IPs, destination
- IPs, and destination ports.
- Allow connections necessary for state online testing systems to function. This should only be
- allowed by destination IPs, and destination ports. See addendum for DRC IPs.
- Once all above actions in Phase Three have been completed and verified, proceed to Phase Four.

Phased Process and Q&A

Emergency Cyber Incident Prevention Critical Task List – Phase 4

- Allow connections necessary for other critical systems to function. This should only be allowed by explicit source IPs, destination IPs, and destination ports.
- **No connections should be allowed to the internet over all ports** (ex. Do not add ‘any any allow’ rules)
- Once all above actions in Phase Four have been completed and verified, proceed to Phase Five.

Phased Process and Q&A

Emergency Cyber Incident Prevention Critical Task List – Phase 5

- Review the ***Preventive Measures Checklist*** and implement where possible. Most importantly, ensure backups are stored in an offline / offsite location.
- Look for signs of infection. The ***Indicators of Compromise checklist*** is a good starting point
  - If signs of infection are found or suspected, contact your OEP director immediately.
- Once all above actions in Phase Five have been completed and verified, proceed to Phase Six.

Phased Process and Q&A

Emergency Cyber Incident Prevention Critical Task List – Phase 6

- Review and update web content filter policies so that connections to uncategorized / unknown websites and websites using IP addresses instead of DNS names are blocked.
- Allow workstations to access the internet through the web content filter, over TCP ports 80 and 443 only. Do not allow any web traffic that did not pass through the web content filter first. **Servers should not have internet access at all.**