Lane County Technical Advisory Committee
Thursday, Oct 23, 2014 1:00 to 2:30 pm
Room 5, Lane ESD, 1200 Hwy 99N, Eugene

Lane County Technology Advisory Committee
MINUTES

PRESENT: Arne Berglund (LESD), Daniele McCallum (LESD), Jason Dodge (LESD), Christina Okesson (LESD), Jacob Shaw (Springfield), Nathan Martin (Bethel), Steve Shininger (4J), David Nelson (4J), Nathan Bowers (Lowell), Jesse Baber (South Lane), Michael Bateman (Fern Ridge), David Bolton (Bethel)

Intro discussion: Dealing with a security breach — Shininger, 4J

Steve shared insights into the June 2012 security breach at 4J. Shared some details on the discovery and investigation, as well as various actions and policy changes implemented and still being refined.

Brief Roundtable and questions:

- Jesse brought up some thoughts on MealTime database security. MealTime will probably force going to Empower soon which moves the database to the cloud.
- Daniele asked about the time-frame from beginning to the call to EPD. Not long. Didn't have much logging on the machines or on the network. Once had circumstantial evidence, it was the next week when they delivered the info to EPD
- Jason asked if there are any local experts when it comes to forensic – Arne said the FBI local office has a forensic specialist. Jacob mentioned Wayne Marnie (sp?) who has helped them with legal aspects. Has anyone had penetration testing done? Springfield had a pen tester come in and he did a great job. Didn't get through the firewall, but he could have. Let him in to test areas. Pen testing with backtrack - $1200 course (offsec.com) with certification. SANS member and forensic expert Hal Pomeranz (Deer Run Assoc.) is also still based in Eugene. Info AtRisk is still in Eugene.
- Jacob asked what 4J is now doing with logging. Have routers at every school, and inside schools not doing a lot of logging. Trying to do better there. Jesse uses NetDisco

Topic of the Month: Firewall, Core Security

1. **Overview/Intro — LESD**

Jason PowerPoint presentation. Districts behind firewall. Bethel, LCC, and Lane ESD are screened, but exempt from policies. Netscreen-1000 ISG, Juniper gear. Built-in VPN, but we don't use it for VPN services. Diagram of core, edge router, ISG-1000s, aggregation switch and router, then CPE. Overview of zones. Snapshot of screening. Reports went out to each district this month – does anyone have any questions or comments? Jesse asked why the password? Extra layer of security. Maybe do a password-protected pdf next time, and not Excel? Many districts had not seen this information. Information about what to include when submitting a policy request. Managing a firewall is an organic process, so our intent was to check in and make sure our staff and districts are still on the same page. Cleaned up quite a few contractor accesses, Pentamation printers, etc. Jason spoke to the idea of "deny" vs. "reject." Jesse has used the Reject on servers. LESD used the Reject for the YouTube issue last spring, to get an immediate result. We can do traffic counters or policy logs, policy scheduling, etc. Looked at an example of traffic counters and also policy logs. Gave an overview of the hardware status and support/maintenance. Looking to put in a new device and would like to work with Springfield and 4J to come up with a good solution.

2. **Best Practices — Roundtable**

What are people doing for VPNs at their sites?

- Bethel has a few Cisco Ethernet clients. Very few. Generic user account that authenticates. Use Aruba remote access points and like them. On a different VLAN.
- Richard using ScreenConnect software at Crow. Most just want access to their machines from their home machines.
- Jesse uses remote access points and web server has SSH. Recommends GoogleDocs for staff. Have a Cisco ASA with VPN for a camera on the radio tower.
- Springfield uses Cisco ASA with VPN, but it is challenging for end users. Maybe a dozen people. Have a hard time with Java clients.

Who are the folks that are approved to access from home?

- Individual requests handled case by case.

Is anyone using software firewalls?

- Jesse mentioned someone left them all on their managed devices. Has been systematically removing.
- Bethel had it disabled, and with new upgrades they have a firewall policy. SystemCenter lets it run very smooth.

Anyone thinking about Intrusion Protection (IPS)?

- 4J has a module for IPS on the ISGs, but not doing anything fancy with it.

What are your responses to a security issue?

- Fern Ridge gathers as much info as he can with logs. Don't have a centralized SysLog. An email went out to all staff about monitoring credit records.
- Springfield – Jacob does forensics. If a crime, he reports to the police. Lock up all equipment to protect while investigating.
- Jesse asked what happens when a district has a sensitive laptop stolen? Experience at South Lane. Eugene has Meraki desk map client installed so that if a machine is booted up and on a network, they can access it and delete, or track it. Springfield has something on the guest account that contacts the district if it is on wifi. Have gotten at least a dozen laptops back. Bethel using CompuTrace for locating. Eugene is mostly OS10, not using Casper yet.

3. **Challenges — Roundtable**

   Michael mentioned that special requests usually are a result of something being flaky, not the firewall. It is very hard to escalate with vendors, he much prefers to work with staff at LESD first.

   Jesse asked about public IP addresses for guest wireless. Is it worth firewalling? Short answer is yes, but LESD doesn't administer districts' wireless. It would make more sense for the district to do something within their controller. You would have to explicitly deny on the other side of your district firewall. Best thing to do is if you see something inappropriate on your network, to communicate to that other site and let them know (they may not know).

   Michael asked how many are using services that are shared/connected with others? Arne said the bulk of cross-district traffic are for districts running their own web servers in-house (South Lane for example). Services from UofO are different, and not shared inside our firewall. Do the large districts firewall in-between schools? No, but Springfield is looking at a gateway firewall and an internal firewall, but don't know if that will happen this year. Eugene is similar – they could, but don't currently.

   Richard asked about secure browsing through TOR? More and more students bringing own devices. Jesse looks at it like CIPA is best-effort. Not much you can do about it if it's on their personal device. Crow is in a unique position because of being in a no-data cell zone. Springfield identifies TOR traffic the best they can, but don't block it. You could identify and sabotage it, but it's a lot of work.

4. **Changes you would like to see — Roundtable**

ADDED ITEMS:

- At the Superintendents' meeting and curriculum leaders meetings administrators went over the Lane ESD Local Service Plan – it is that time of the year to let us know what your needs are. Technology piece – pilot for tech services project in JC was last year. If your administrators talk to you about anything, that is the context. Nathan asked about group purchase of Aruba AirWave? Had a presentation in the spring, and didn't really go anywhere. Daniele can send out an email to see if there is any interest. Would need to collect number of APs (not Aruba-specific) if you are interested.
- Daniele asked about purchasing philosophies for smaller items. Do you have a standard to help you with decision-making? Richard's email about headsets – was a good thread. Go with the best-value before the lowest-cost. David Bolton will forward email from Troxell. Do you want a purchasing discussion included with LCTAC, or through email? Jacob likes email, because of the conversation history log. Maybe an occasional overview of the top things. Maybe a blog so that it is all in one spot?
- Arne mentioned a message going out next week discussing access to the filtering reporting interface, for districts using LESD filtering.
- Filter changes at Bethel – illegal music downloads and couldn't track it down. Added to syslog server. Changed Lightspeed peer-to-peer settings.
- Nathan asked if anyone is using Port Security? Bethel is implementing in the near future. Jesse mentioned a product called Packet Fence.

Next planned LCTAC meeting, Nov 20, 2014

Topic – Email systems