Community Expectations for Campus Computer and Network Security BoF

Joe St Sauver, Ph.D.
joe@uoregon.edu or joe@internet2.edu
Internet2 Nationwide Security Programs Manager

Tuesday, July 13th, 2010, 4:30-5:30PM
Internet2 Joint Techs
The Ohio State University, Suzanne M Scharer Rm, 3rd Floor

http://www.uoregon.edu/~joe/comm-expect/

The Original Campus Expectations Task Force

- The original charge for the Campus Expectations Task Force (CETF), circa 2005, was described by Bill Decker, head of the Task Force in a talk he did for the Fall 2005 Internet2 Member Meeting, see www.internet2.edu/presentations/fall05/20050920-cetf-decker.ppt

  Articulate a current set of expectations for what it means to be an Internet2 member campus.

  - *Consider focusing on what the campus infrastructure needs to be 2-5 years out in order to support advanced applications.*
  - *Areas considered should include campus network configurations, campus directory implementations, privilege management, data storage, image transfer/management, computation,* ***security,*** *campus bandwidth management, collaboration environments, and others.* [JES-emphasis added]
  - *Consider the responsibilities that come with supporting sponsored participants and SEGPs.*
  - *A series of case studies that illustrate the best practices of campuses in resolving these issues will also be created.*
  - *Seek input from a broad range of constituency groups, including but not limited to CIOs, application developers, GigaPoP operators, network engineers, support staff, faculty, researchers and other users.*

Expectations Function #1: Minimum Standards

- It was clear by 2005 that it made little sense to have a high speed nationwide backbone (such as Internet2), if existing campus or regional networks were slow and congested, or if key servers and researchers were only connected via 10Mbps chokepoint links.
- Put another way, if you made the effort to connect to an advanced national R&E network, other sites might reasonably expect that your network had more than just "vanilla IPv4" capabilities, perhaps including the ability to support advanced network protocols such as:

  -- IPv6,
  -- IP multicast, and
  -- jumbo frames (e.g., 9K MTUs)

Expectations Function #2: Keeping Us All Stretching Just A Bit

- The CETF process was also envisioned as serving an important "forward looking" role, going beyond just saying "where should we be now?" to laying out "where should we be two to five years from now?"
- In the simplest of terms, if campuses had 100Mbps backbones in 2005, we needed to be actively working to get upgraded to gig backbones, while planning for 10 gig backbones (and maybe even doing basic research needed to make 100 gig backbones a reality when they're needed)
- The general expectation was/is that we should be "challenging" ourselves at least just a little; Internet2 shouldn't be just about living comfortably at a currently adequate but not exceptional level.

Note: Not All Expectations Were Purely Technical

- While some expectations were technical, others were not.
- One might also expect organizational commitment to advanced networking, including support from institutional executive management, appropriate institutional financial commitments, commitment of personnel and facilities, etc.
- Metaphorically, if you were going to be part of the "club," you were expected to actively participate, making a reasonable effort to "stay up with the pack" and to contribute to advancing the good of the order.
- Explicit articulation of community expectations has the potential to serve an important normative function, allowing people to identify areas where success has already been attained locally, and areas where more effort is still required.

Expectations Also Served to Reassure

- For instance, note the explicit reference to supporting SEGPs and sponsored participants in the original charge.
- At the time that charge was prepared, there were worries that when Internet2 allowed connection of state K12 networks (as SEGPs), or smaller institutions with less of an instituional emphasis on advanced networking (as sponsored participants), that that step might result in the creation of substantial new operational burdens, burdens which might be born by the community as a whole rather than by the sponsored or sponsoring site.
- Of course, in retrospect, we know that anticipated deluge of potential problems didn't occur, but at the time, some were worried and wanted reassurances.

Expectations Also Were Meant to Educate, And To Be Demonstrably/Provably Attainable

- In particular, the case studies mentioned in the charge were meant to illustrate how members of the community were actually meeting the community's articulated expectations, thereby showing peer institutions at least one proven path that presumably could also be replicated by others.

- "Let me show you what we did. When you check out what we did, you'll see that it's worked well for us."

- Those are the sorts of things that were originally envisioned (or at least that's my recollection)

The CETF Final Report Was Issued Spring 2006

- A final report from the CETF was produced in Spring 2006, and remains available online at http://www.internet2.edu/files/CETF-FinalReport.pdf

- A discussion of that final report is also available, see http://www.internet2.edu/presentations/spring06/200604225-cetf-decker.ppt

- Somewhere along the line, though, we all got a little distracted, and work on shared community expectations got postponed or deferred, even though the need for shared community expectations was ongoing.

Fast Forward Now to The Fall of 2009

- In the Fall of 2009, during discussions of the Internet2 Salsa Security Advisory group, the issue of community expectations came back up, with input from Salsa members including members of the Applications, Middleware and Services Advisory Council.

- Consistent with Tasks G ("Implement Security Best Pracatices") and J ("Cooperate on Security Challenges"), of the Internet2 Strategic Plan, Internet2 has been working with Educause and the REN-ISAC in providing **security information** to our colleges and universities.

- But that information is just that: **informative/descriptive**, rather than **normative/prescriptive.**

"A Normative Campus Security Agenda"

- In May of 2008, for the Educause Security Professionals Meeting, I put together a presentation called, "A Normative Campus Security Agenda," see www.uoregon.edu/~joe/spc2008/security-professionals.pdf

- That list of normative activities included things such as:

  -- have antivirus
  -- respond to incidents
  -- have a campus AUP
  -- etc.

- But that was a LONG document, 103 slides, and frankly, probably just too dang long for folks to pay attention to.

How About A Much Shorter List: Just Ten Items

- Coming back from the Fall 2009 Internet2 Member Meeting in San Antonio, I snagged my colleague Dale Smith from the University of Oregon to help, and together we came up with a list of just **ten items** that one might take as a starting point for basic Internet2 community expectations relating to security.

The Ten Items That Dale and I Came Up With

- 1) Have a cyber security officer/group
  2) Have a cyber security plan/acceptable use policy
  3) Site license an antivirus software product
  4) Participate in the REN-ISAC
  5) Have an intrusion detection system (Snort, Bro, etc.)
  6) Be able to translate a reported IP address to a MAC address to a switch port to a machine/person (even if there are NAT related complications involved)
  7) Route traffic on campus, don't just switch
  8) Locally firewall important assets and provide encrypted VPN access
  9) Eliminate clear text passwords (telnet, ftp, pop, imap, unencrypted administrative web applications, etc.)
  10) Work on identity management/some sort of centralized authentication

The Spring 2010 Internet2 Member Meeting

- As much as I liked that list, :-), we wanted to get some feedback from the community.
- We had a BoF-like session talking a little about this topic during the Spring 2010 Internet2 Member Meeting in Arlington VA.
- A number of themes emerged from the brainstorming which we had there, and I'd like to take a couple of minutes to recap those briefly today.
- Note that these themes reflect the opinion of individual audience members, and if you were at the meeting and I've mis-summarized what you were trying to say, please give me feedback so I can get the record corrected. :-)

Some Potential Higher Level Expectations/Principles

- Rather than drilling down too specifically, one contributor suggested focusing on higher level expectations/principles:
- Don't hurt me!
- Use security mechanisms that don't break cool stuff (multicast, ipv6, etc.)
- Share with your friends (security info, incidents, etc.)
- Think about the function that security should be facilitating -- facilitate useful things, don't just prevent bad things
- Seek out and implement best practices
- Have a light touch.
- Other audience members had very specific suggestions…

Example of Specific Feedback On One Concrete Issue: The Campus IT Security Office

- Each site should have a Security Office/Officer
- Most sites hould have a *Formal* Security Office; some sites have casual/part-time/distributed informal security office(r)s
- Needs well trained staff
- Should have specific security goals
- Needs to have security policies, and the authority to enforce those policies (some folks already have this, some don't)
- Must have an adequate budget for security
- Should join REN-ISAC

General Goals/Considerations Feedback (1)

- Apply service management principles (SLAs, definition of the services, ITIL, service management lifecycle)
- Collaborate on security; not just everyone for themselves (work between schools, not just within each site)
  -- Can motivate/drive evolving model for data collection and sharing
- Consider a tiered approach (basic sites, mid-tier sites, advanced sites)
- Create sample policies that people can use as a foundation
- Encourage dherence to BCP's (including things such as ARIN contact points, BCP38, no open recursive DNS servers, etc.)

General Goals/Considerations Feedback (2)

- Internal Audit -- connect the policies, insure that departments use those policies
- Manage your network borders
- Minimize likelihood of damage from security incidents that might have been avoidable with training, etc. (DMCA perhaps, inadvertent loss of PII)
- Need management understanding of risk; risk isn't just an IT issue
- Network neutrality dangers (risk of loss of ability to manage network; countervailing/concurrent risk of loss of network transparency)
- Policies and mechanisms to implement policies (e.g., procedures) can be, and should be, seperated

General Goals/Considerations Feedback (3)

- Prepare campus members (e.g., undergrad students) for their eventual professional lives (including helping them understand that Facebook content (even goofy content) is forever!)
- Rank the priority of the items to be accomplished
- Recognize differing constraints: (budget limits, personnel limits, etc.)
- Recognize that some security policies/techniques may be more durable than others -- some security policies/techniques may address short term issues, others may have a longer term/more strategic value
- Risk assessments should be getting routinely performed

General Goals/Considerations Feedback (4)

- Security planning for applications should happen before they're deployed (not afterwards!)
- Security review/security considerations should be part of the procurement process
- Test your security protocols/security measures
- Training
  -- Needs to be valuable to users
  -- Education and Awareness component for security programs
- Understand, segment and secure sensitive data and applications

Some SPECIFIC Security Technologies Which Were Mentioned (1)

- Ability to block or sinkhole malicious network traffic (IPs, URLs, addresses, etc.)
- Antivirus
- Consolidated syslog
- DNS (DNS logging, DNSSEC, etc.)
- Identity Management:
  -- Easy to use, easy to administer PKI
  -- Have Good Identity Management
  -- Shibboleth and InCommon
- Incident Tracking System
- Netflow collection

Some SPECIFIC Security Technologies Which Were Mentioned (2)

- Patch Management
  -- Patching policies
  -- Patch level monitoring for installed applications (beyond OS and Office, etc.)
- Systems:
  -- Information Assurance Hardened Servers and Desktops
  -- Have an IT person responsible/desigated for each system who *understands* that system! (e.g., not a Mac person for a Windows system or vice versa)

Narrowing in On The <N> Key Security Items

- I had one person tell me that if you want to get down to ten items, one good way to get to ten is to ask for no more than three. :-)

- So what are the **three** items you'd like to see as security expectations?

  1)

  2)

  3)

Next Steps

- Unlike some security sessions, today's session wasn't meant to unveil a completed product, ready for broad adoption, it was just meant to introduce the topic and set the stage for ongoing community discussions, and to begin getting some input from you.
- We want and need to hear from <u>you</u>, Internet2's members, about what <u>you</u> think our community's collective security expectations should be -- after all, these are supposed to be COMMUNITY expectations, right? :-;
- If you're potentially interested in working on this topic, please send me an email at joe@internet2.edu or joe@uoregon.edu
- Do we want a mailing list?