Task G: Implement Security Best Practices (DRAFT, 4/16/2009)

G. Develop and promote cost-effective methodologies, standards, and best practices for security and end-to-end application performance. Implementation must be possible under real-world conditions across campus, regional, national and international networks.

Environmental Scan

- The number one IT issue for higher ed CIOs in 2008 was "security." "Identity/access management" and "disaster recovery/business continuity," two addtional areas intimately related to security also appeared on the Educause CIO "Top 10 IT Issues" list, checking in at fifth and sixth place this year.

- Bots (Windows PCs which have been hijacked via computer viruses) remain a key enabling technology behind many cyber threats. Bots are routinely used to deliver spam, phishing, and malicious software (malware). As MS Windows, Internet Explorer, and MS Office have become more bug-free, attackers have turned their attention to "helper applications," exploiting unpatched bugs in software used to display PDF documents or digital movies. PCs running Windows can get infected even with fully-up-to-date antivirus (A/V) software. Up to 50% of all malware isn't detected by A/V software at the time that the malware gets disseminated. Fake A/V products (providing misleading "detections" of non-existent infections) are now also very common, causing (rather than eliminating) infections when users get tricked into trying them.

- Unauthorized disclosure of PII (Personally Identifiable Information, such as Social Security Numbers) remains a huge and potentially career ending concern for CIOs at many sites. PII on administrative systems and PII in data obtained for research purposes by faculty members can be equally problematic. Many PII spills are the result of miscreants exploiting longstanding vulnerabilities in web applications. Other attacks continue, but web application vulnerabilities represent an important and fast moving new "front" in the online war being waged against us.

- Flaws in critical foundation protocols are also increasingly under attack. For example, attacks on the domain name system (the key Internet background service that translates site names such as www.google.com into IP addresses such as 74.125.19.99), have become more common. Solutions to these vulnerabilities in critical foundation protocols are known, but deployment of those solutions can lag at sites which are overwhelmed just trying to "put out fires."

- Another example of a key security-related area is identity management, where the need to make progress on scalable federated solutions is great but the resources for successful project implementation may be unavailable at some sites. Because of the central role that identity management plays, the community might want to consider identity management (and the scaling and privacy challenges it addresses) as a separate focus area rather than simply a major aspect of security.

- Regulatory compliance burdens are increasing, diverting critical technical security staff and driving campus network architectural decisions in ways which may be fundamentally incompatible with advanced applications and high performance networking. For example, while perimeter firewalls have been widely deployed, security based on perimeter firewalls isn't the only option higher ed can or should consider. Academic research should support and be supported by investigation of alternatives to perimeter firewalls.

- A final environmental factor worthy of note is that the Internet2 community collectively controls some extremely powerful networks and systems. With that great power comes great responsibility. All the networks that connect directly to us, and the Internet as a whole, implicitly trust our community to be responsible stewards of those capabilities and resources, securing them from being diverted, misused or abused. Our ability to continue interacting with the global high performance networking community is preconditioned on our living up to that trust.

Current Support

Internet2 currently has < 1.5FTE devoted to security programs. Most of that security FTE is distributed (campus-based), rather than centralized at Internet2's offices in Ann Arbor. Internet2's Security Program provides detailed practical guidance and thought leadership on both current and emerging security issues, including security best practices needed to ameliorate security issues while maintaining a high performance, easy-to-use, and easy-to-support network. Guidance is shared via:

- Delivery of formal presentations; participation in panels, BOF sessions, and working group sessions; and service on program committees for a variety of events including *inter alia*:
    - the biannual Internet2 Member Meetings and Internet2/ESnet Joint Tech Meetings,
    - the EDUCAUSE annual conference and the EDUCAUSE Security Professionals Meetings
    - relevant national and international security events
- Participation on/in/with:
    - Salsa, Internet2's long-standing security advisory group
    - the Internet2/EDUCAUSE Security Task Force Leadership Team
    - the Research and Education Network Information Sharing and Analysis Center (the REN-ISAC), including work on the REN-ISAC Technical Advisory Group and work on the REN-ISAC Executive Advisory Group
    - Educause's Security Effective Practices working group, including former service as co-chair of the Security Effective Practices working group
    - federal agency cyber security R&D roadmaps and planning activities
    - site security reviews
    - community security-related mailing lists and conference calls, as well as one-on-one work with members by email, phone, etc.
- Grant funded research on security incident information sharing and collaboration.

In all of that work, we're acutely conscious of the ongoing need for recommended solutions to be practically deployable and cost effective, while also being solutions which will fit well with higher education's unique culture.

In general, we do our best to concentrate on timely security issues which will need community attention and action within a one to five year time frame.

Possible Future Activities

In response to an earlier request from Internet2's Senior Director for Middleware and Security, we'd prepared a brief table of twenty possible future security topics for consideration and review by AMSAC at the 2008 Internet2 Fall Member Meeting (see http://www.uoregon.edu/~joe/security-tasks.pdf). AMSAC reviewed and discussed that table during the Fall Member Meeting. We also shared a pointer to that table (and an explicit request for feedback about it) at the Security Activities Update session at the Joint Techs Meeting in College Station TX during February 2009. As part of our ongoing work, we've begun to tackle priority areas from that table. For example, at Joint Techs we presented work on the "IPv6 and Security" topic from the table, and work on "Domain Names, IP Addresses DNS and DNSSEC" is also ongoing, including work with ICANN on the fast flux problem.

Given the important role of the Internet2 Dynamic Circuit Network (DCN), we also need to work through and understand the security implications of DCN-type facilities. We know that at least some interest in DCN is motivated by the desire to get a "clean network path" which is unencumbered by campus firewalls and other security middleboxes. Also related to DCN, security of the dynamic circuit control plane is another new dimension which we must also analyze, including scrutinizing the security

of circuit signaling across multiple independent domains (e.g., the Internet2 backbone network, regional optical networks, campus networks, etc.). There's also interest in understanding the security implications of cloud computing, outsourcing, and community based distributed initiatives (such as GENI, the Teragrid, and the Open Science Grid, among others).

The Campus Expectations Task Force will play a critical role in helping the Internet2 community attain a common minimum security "baseline." By developing appropriate community-wide security norms, we'll be able to help our community enjoy real cyber security while still retaining the inter-institutional ability to do advanced networking tasks (such as high speed bulk dataset transfers; the use and investigation of advanced protocols, applications, and architectures; and the ubiquitous deployment of supporting collaborative tools such as interactive video).

Metrics for Success

Ultimately, the one true metric for the success of any program, whether security-related or other, is the degree to which it meets the needs of its customers. We suggest that Internet2 employ focus groups to better understand the security needs of its members, including obtaining feedback on security areas where the community may have unmet needs.

If asked to provide a concrete example of a successful Internet2 security initiative, we might point to the work of the Internet2 Salsa-DR (Disaster Recovery Working Group) in the period immediately following the terrible tragedy at Virginia Tech. Coincidentally, Salsa-DR was scheduled to meet during the Spring 2007 Member Meeting, and during that meeting information about the need for institutions to be ready to provide real-time notifications to their users under the federal Clery Act, including information about how schools could practically accomplish this, was shared. Today, virtually every Internet2 university has taken steps to become Clery Act compliant, with many choosing to deploy so-called "reverse-911" systems capable of pushing emergency communications directly to faculty, staff and student cell phones. That, we believe, is a prime example of a successful security program meeting both a genuine need and a compliance objective at the same time.

Other processes, such as working to insure that well-intentioned security measures are architected in ways which won't make it impossible for users to do their work, may be harder to quickly tally, but are no less important for their incremental impact or the harms they quietly help prevent.

Contacts

If you have feedback on this document, please contact Joe St Sauver, Manager, Internet2 Security Programs (joe@internet2.edu or 541-346-1720)

References

"Top 10 IT Issues, 2008," *EDUCAUSE Review,* vol. 43, no. 3 (May/June 2008), pages 36-61. http://tinyurl.com/EducauseTop10List2008