OARsec Meeting Minutes

21 October 2015

BALE Theater, OARnet, 1224 Kinnear Rd, Columbus OH 43212

Attendees: 32 attendees registered

Meeting Notes: scribed retrospectively by Mark Beadles mbeadles@oar.net

Minutes

Meeting was called to order at 1:00 by Mark Beadles, OARnet. Mark noted that the previous OARsec chair, Matt Dalton of Ohio University, is no longer with the University, leaving the member chair currently unoccupied.

Mark Beadles and Kevin Nastase, OARnet, gave updates on OARnet's Federated Identity Management and DDoS protection programs.

Federated Identity

"IAM Ohio" is OARnet's branding of a service package for enabling federated access. OARnet members can contact their client service representative to request these services. Member funding has helped OARnet make a set of federated services available which include:

1. Identity Provider (IdP) server software packaged as a VM, supporting InCommon (http://incommon.org) and eduroam (http://www.eduroam.us/)
2. OARnet-hosted RADIUS proxy servers supporting eduroam
3. IDM Installation/Implementation/Design services
4. Pre-approved InCommon Federation participation agreements for Ohio institutions (http://www.incommonfederation.org/iamohio/)
5. Eduroam registration and administration

DDoS Protection

Distributed Denial of Service attacks were noted as a growing concern, especially by the larger institutions. Mark and Kevin explained that OARnet has the ability to assist in DDoS response by applying certain measures upon client notification, including application of rate limiting or RTBH (remotely-triggered black-hole routing). Additionally, upon client request, OARnet has the ability to proactively put in place rate limiting for protocols commonly used as vectors for DDoS (e.g. UDP reflection attacks). OARnet is also piloting and/or investigating additional potential solutions including hybrid cloud-scrubbing services, and the use of BGP Flowspec (RFC 5575).

VENDOR BRIEFS

The group expressed interest in aggregate pricing for certain security-related vendors. Vendors with current higher education or State pricing include the following, with links to pricing information. No endorsement is implied other than providing information on pricing.

- Duo (2-factor authentication)
  http://www.incommon.org/duo/fees.html
- Splunk (SEIM/log management)
  http://www.internet2.edu/products-services/cloud-services-applications/splunk/#service-fees
- Palo Alto (NG firewall)
  http://www.immixgroup.com/uploadedFiles/Documents/Products_by_Contract/534103_878.pdf
- SANS Securing the Human (User and Developer Security Awareness Training)
  Note: discount purchase window ***December 1, 2015 - January 31, 2016***
  https://www.securingthehuman.org/pricing/education

EDUCAUSE AND REN-ISAC REPORT

Previously in the week, Joanna Grama of EDUCAUSE discussed security issues in higher education with the OARnet CIOs. Mark shared some highlights of her presentation. The full presentation can be found on the OARsec site: https://oar.net/about/oarsec/presentations. Some highlights:

REN-ISAC

http://www.ren-isac.net/

Research and Education Networking Information Sharing and Analysis Center

- Cybersecurity operational protection & response in research & education community
- Private information sharing in community of trusted representatives at member orgs
- Computer security incident response team (CSIRT)

EDUCAUSE HIGHER EDUCATION INFORMATION SECURITY COUNCIL (HEISC)

http://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-initiative

Information security governance, compliance, data protection, and privacy programs

- Information Security Guide
- Case Studies
- Toolkits
- Resource Library
- Awareness Tools
- Toolkit for New CISO's

SECURITY PRIORITIES FOR 2016

The group shared its priorities for 2016. The most noted items for the group were:

1. Phishing protection
2. Shared vulnerability scanning service
3. Adoption of Eduroam shared wireless
4. Implementation of next-generation firewall
5. End-user awareness training

Election of Member Chairperson

No member in attendance volunteered to be nominated for this position, so a public call for nominations will go out soon.

Adjournment

Meeting was adjourned at 3:00 pm.