Minutes from I.T. Council meeting 2/20/17
Travis Conference Room, Bizzell Memorial Library

Attendees

Patrick Livingood, Co-Chair – Anthropology
Carl Grant, Co-Chair – OU Libraries
Stephen Crynes – UC Major Exploration
Elizabeth Pober – Architecture
Aaron Baillio – IT
Ron Fellhauer – IT
Tim Marley – Internal Audit

Anna Biggers – IT
Burr Millsap – Administration & Finance
Aaron Biggs – Provost Office
Loretta Early, IT
Eddie Huebsch, IT
Boris Apanasov – Mathematics

Meeting called to order by Patrick Livingood at 10:30

- Minutes accepted and seconded.
- Loretta - Password Change / RansomWare
  o Several thousand passwords changed over last weekend.
  o Down to relatively few.
- Ransomeware by Ron Fellhauer
  o First occurrences in Russia in 2005
  o Attacks have grown by 600% since Dec 2015
  o HealthCare especially hard hit.
  o Are encrypting master boot record, takes about 1 second
  o Symantec sais 35-40K systems are infected with ransomware each month
  o 5% of impacted organizations pay the ransom.  Ransom payments will reach $1b in 2017
  o Some varieties exfiltrate data prior to encryption
  o Phishing = ransomware.  93% of phishing emails contains ransomware payloads
  o Proof point estimates that 83% of ransomware is initiated by email links, attachments or website downloads.
- Defensive measures
  - train users to recognize phishing
  - Use email gateway to scrub attachments and links
  - Backup often and test recovery
  - Patch known vulnerabilities to limit spreading
  - Develop a response plan
    - what criteria do you use to make decisions
    - Can you recover, what resources are needed
    - Will you pay?  How?
    - Use email gateway if possible. (we are at OU).
    - Recovery plan in place?  Can you switch to secondary systems?
    - Ransoms are typically paid through a BitCoin account.  Not easily set up. Some orgs are setting up BitCoin accounts.
Current Defenses
- Proof point examines all attachments and r-writes malicious URL
- Next Generation FWs block traffic to know malicious networks
- OpenDNS blocks request to known malicious addresses
- New DDPE on endpoints is 95%+ effective at detecting ransomware on endpoint.
- AlienVault and Damballa tools to id and alert malicious payloads
- Network segmentation allows for containment of malicious traffic
- ComVault tool provides backup and recovery
- Office 365 and OneDrive can provide backup.

More opportunities
- More training and awareness
- Formal incident response plans
- More vigilant patching cadence
- Expanded log capture and review
- Better asset tracking and management
- Cyber insurance.
  - OnPoint has a course to train people (Patrick will send link)
  - Ron can help you set up a phishing test for department.

- OnePortal
  - Faculty experience is being worked on. Working through checklist before Ozone is shut down.

- ProofPoint
  - Aaron Baillio
    - Timeline
      - Feb 2016 - All 3 campuses hit by ransomware, delivered by email
      - In response we blocked certain file types
      - Mar/Apr 2016
        - Conducted a solicitation of other peer research institutions on email security
      - May 2016
        - Recommendations to Risk Review Board for email security gateway
          - Peers were doing some level of email filtering
      - June-Nov 2016
        - Researched gateway providers
        - Researched integrations and proof of concept
      - Dec 2016 C
        - Contract negotiated
      - Feb 2017
        - Cutover
      - Total mail volume/week is 3-4M
      - 300-400K spams were being blocked using O365 filters
- Proofpoint is knocking it way down.
  - Stats
    - 15M emails being processed. Nearly 1/2 is being hard-blocked by ProofPoint.
  - Advanced Threat Protection
    - Where sandboxing or rewriting URL’s
    - 91.3% are being blocked successfully.
  - Biggest wins?
    - Finer control over spam filters
    - Better detection and prevention of true threats
    - Detection of abuser or compromised accounts
    - Correlation with CloudLock/Open DNS
  - Issues/Opps
    - Legacy on prom email servers
    - No policy governing independent email servers (role for ITC??) Majority of outgoing spam is coming from these machines.
    - False positives?
      - Difficult to determine % but suspect it is low
      - Continue to tune policy
      - Message quarantine digests
    - May set up an email digest or a portal for users to check and see what is blocked.
  - Open Discussion
  - ITC Charter
    - No comments.
    - Move to accept ITC charter by Carl Grant, seconded by Elizabeth Pober.
  - Acceptable Use Policy
    - Patrick raised issue of Supervisors to ensure reporting staff to be informed and assured of knowledge of policy
    - Students records/email seem to be exempt from much of this. Are we viewed as ISP provider to our students (we are) but not clear if we’re regulated as other ISP’s.
    - May need to formulate our list of questions and then have IT sit down with legal.
    - Deferring discussion and collect questions for next meeting.
  - Meeting adjourned at 11:30 am.