CEHD Information Security Procedure
IS-7 IT System Monitoring

Procedure Statement

The purpose of the information system monitoring policy is to ensure that 1) information systems are regularly reviewed to identify problems and vulnerabilities as soon as possible so as to mitigate the consequences and 2) appropriate security controls are in place.

TAMU Security Catalog SI-4 Information System Monitoring[1]

TAMU Security Catalog AU-2 Audit Events[2]

Procedures

System Logging

The CEHD has implemented GrayLog, an open source log aggregation server, to continually pull logs from CEHD servers into a form that can be easily queried.

1. GrayLog is the method the CEHD uses to monitor security logs.
2. All production servers shall be configured to use GrayLog for security logs.
3. File servers that manage confidential data shall be configured to record object-level access to files. These logs shall be included in GrayLog.
4. Logs shall be maintained within GrayLog for 30 days.
5. Naemon shall monitor the GrayLog storage and alert IT staff when the disk usage exceeds 90%.
6. In the event that the GrayLog disk usage exceeds 90% (and it is determined that the increase is not a unique event), the storage space for GrayLog shall be increased.
7. Queries shall be developed that will allow for easy monitoring of critical errors.
8. Designated Technology Services personnel shall review GrayLog on a regular basis.
9. Systems designed as containing confidential information shall be configured to enable object-level logging.

System Monitoring

The CEHD has implemented Naemon, an open source monitoring tool, to monitor specified activity on CEHD IT systems.

1. All production servers shall be configured to report critical events to Naemon.
2. All critical services within each server shall be monitored by Naemon.
3. Naemon alerts shall be sent via e-mail to the appropriate IT personnel.

Security Policy Monitoring

- Server patches. Technology Services has implemented an internal system to remind server administrators monthly regarding server patches.

Windows Workstations

CEHD set the security log size for Windows workstations to be 20 MB.

[1]TAMU Security Catalog SI-4 Information System Monitoring
http://cio.tamu.edu/Risk_Management_Policy/IT_Policy_Compliance/PDFs/SI4_Information_System_Monitoring.pdf

[2]TAMU Security Catalog AU-1 Audit Events
http://cio.tamu.edu/Risk_Management_Policy/IT_Policy_Compliance/PDFs/AU2_Audit_Events.pdf

Revised Janurary 18, 2017