SAND2011-7911P

Data Loss Prevention

Data Protection

- A concentrated focus has been placed on ensuring and improving the protection of unclassified, sensitive data (such as Personally Identifiable Information (PII))

- Data Loss Prevention (DLP) was selected as one method for protecting data

- Data Loss Prevention is the practice of identifying and protecting sensitive data from unauthorized use and transmission.

DLP Tool Evaluation and Selection

- Completed a tool evaluation and select a DLP tool
  - Solicited and received quotes for DLP tools
  - Evaluated comprehensive DLP Tool suites from two vendors
  - Both tool sets met mandatory requirements
  - Selected Tool Suite

- Technical and cost benefits of selected tool
  - Capability to configure scanning processes to minimize the performance impact on the system and clients.
  - Incremental scanning – All data is scanned once, but in subsequent runs only new or changed data is scanned.
  - Vendor partners with Microsoft on integration with MS Rights Management (we have a high proportion of MS infrastructure)
  - All communications between sensors are encrypted with SSL
  - Provides extensive hands-on consulting to define policies, configure and install the product
  - Lower cost

Data Loss Prevention capability focus areas

- The DLP tool will include capabilities to identify sensitive data and provide automated remediation actions on
  - data in motion (network); outbound traffic – email, proxies
  - data at rest (datacenter); in storage on corporate files systems and databases
  - data in use (endpoint); on individual client desktops

- Remediation Actions will be automated through the DLP tool.
  - Delete
  - Encrypt in place
  - Move to secure location
  - Quarantine
  - Block

Accomplishments

- Coordinated with subject matter experts from across IT disciplines (system admin, DBA, proxy, email, etc.)
- Implemented the Datacenter component to scan key corporate file systems on a periodic basis for some PII data.
- Implemented Network component to scan unencrypted, outbound email and proxy (web) traffic for some PII data and some specific Official Use Only (OUO) data.
- Partnered with CIO representatives to define policies/procedures to support scope of scanning activity and mitigation processes
- Developed and implemented Communication Plan to provide information to the work force, including a DLP website
- Coordinated with Help Desk organization to provide first line support
- Established Production capability and transitioned completed components
- Developed processes to accommodate requests for service and continuous enhancement
- Conducted first pilot for desktop component in a key business area for protection of PII data; preparing to conduct second pilot
- Conducted Lessons Learned

Future Phases of DLP tool implementation

- Developing plans for additional phases

- Continued transition of completed capabilities to “production” organization

- Potential Phases:
  - Expansion of scanning to include additional PII attributes
  - Expansion of scanning to include additional OUO data (e.g. Export Controlled, Proprietary)
  - Implementation of the Desktop capabilities
  - Expansion of Datacenter scanning to additional repositories
  - Expansion to other networks