Implementing security from the inside out in a PeopleSoft environment

System hardening with reference to the additional concern for insider threat

PeopleSoft supports end to end encryption: browser to web server; web server to Java container; Java container to Tuxedo app server; Tuxedo app server to DB

Security Hardening recommendations, Hosted, On-Premise or Cloud based Systems

Note: This is not a comprehensive list, but a set of basic considerations and not intended to replace a comprehensive security audit

- **Server Room lock down**
  (Key card in and out, no tail gating)
- **Restricted OS CLI** (command line interface or shell) access to DB servers
- **DB Lockdown**
  http://www.oracle.com/technetwork/articles/index-087388.html
- **Transparent Data Encryption**
  (Oracle DB encryption for data-at-rest protection, Microsoft has similar functionality for SQL Server)
- **Review features of Oracle Audit Vault** especially for abusive data harvesting
- **SQL Net traffic encryption** App Server to DB
- **Restricted OS CLI** access to App servers
- **JOLT traffic encryption** Web Server to App Server
- **Restricted OS CLI** access to Web servers
- **Weblogic Lockdown**
  http://docs.oracle.com/cd/E15523_01/core.1111/e12889/infrahard.htm
- **Restrict access to Weblogic Console**, e.g. enable it only when necessary
- **ERP Firewall** which additionally tracks User ID access attempts logging “finger print” data: e.g. workstation ID, User ID, real IP address, user agent, referrer name
- **Separate Weblogic Java container from HTTP Server**, installing HTTP Server in DMZ
- **Risk and Security analysis server** like Oracle Adaptive Access Manager
- **Firewall and Router policies** which restrict internal access to approved web server and proxy addresses, reduced/restricted port 80 enabled or accessible internally
- **HTTPS rather than HTTP by default internally**, PeopleSoft supports SSL 3.0 and TLS 1.1
  (as a result of POODLE threat, eliminating SSL 3.0)

All Security relies on Process, People and Technology

Implementing security from the inside out in a PeopleSoft environment

System hardening with reference to the additional concern for insider threat

- **Software asset management** to retrieve details of software installed on each server/workstation and company owned end user device.
- **Policy lockdown of workstations** to prevent unauthorized installation or unapproved use of USB flash drives, unapproved software, no rogue proxies or TCP/IP traffic sniffers
- **Policy management of end user device** e.g. to ensure current anti-virus/malware software
- Ad hoc and regular **discovery of wireless access points**
- **Uncontrolled use of cloud storage from inside the firewall**
  Document protection and inappropriate sharing
- **Site and web server access protection workstation software**, like McAfee SiteAdvisor
  http://www.mcafee.com/us/products/siteadvisor-enterprise.aspx#vt=vtab-FeaturesBenefits
- **Browser lockdown** by Microsoft policy management to white list approved web servers internally and externally. No local user administrator access.
- **Configure PeopleSoft (or access system) password controls,** e.g. for complexity, length, expiration, consecutive failures.
- Ensure **Node Passwords** are maximum length and complex
- **MDM/MAM** for mobile device access, especially BYOD
- **Use robust Kiosk software for open area access to sensitive data**
- **Use SPF/DKIM/DMARC to protect mail servers (phishing protection)**

Review:

Securing Your PeopleSoft Application Environment
http://download.oracle.com/peopletools/documents/Securing_PSFT_App_Environment_May2010%20v4.pdf

PeopleTools CPU analysis and supported versions of PeopleTools
https://blogs.oracle.com/peopletools/entry/peopletools_cpu_analysis_and_supported

PeopleTools version end of support/life and PeopleTools support for applications
https://blogs.oracle.com/peopletools/entry/peopletools_version_end_of_life

PeopleSoft Technology and Security Video Overviews
https://www.youtube.com/user/PeopleSoftTechnology

All Security relies on Process, People and Technology

Implementing security from the inside out in a PeopleSoft environment

System hardening with reference to the additional concern for insider threat

Questions for the IT/Security Team

- **Do you encrypt data in the database (data at rest)?**
  PET, TDE, SQL Server Encryption

- **Do you use full transport, browser to disk, encryption (data in flight)?**
  PeopleSoft supports Browser to Web Server HTTPS, Web Server to Servlet HTTPS, Servlet to Tuxedo JOLT Encryption, Tuxedo to Oracle DB with Encrypted NetSQL

- **How do you protect against abusive or inappropriate access by high privilege DBA's?**
  Do all DBA's use their own user ID or a common ID for administration?
  Oracle Audit Vault, Oracle DB Vault, other audit (PeopleSoft, GRC, …)
  How quickly can you revoke access, one user, groups of users, high privilege users?

- **How often do you, or do you have a process to, run background checks on employees handling customer data?**
  Internal processes, Attestation, HireRight …

- **How do you protect firewalls, proxies, and IPS/IDS?**
  Do you have different set of credentials for administrator right on each?
  Infrastructure

- **Does your Disaster Plan have a contingency for when a breach occurs?**
  Who makes the decisions to lock down systems, turn off web servers?
  Oracle Rightnow, Content Management, other process automation

- **Do you have a disclosure plan and are you prepared for credibility/reputation loss?**
  Oracle Rightnow, Content Management, other process automation

- **Have you established Security Processes and a defined review cycle?**
  Oracle Rightnow, Content Management, other process automation

- **Do you use Anonymous BIND on Exposed LDAP?**
  Infrastructure

NOTE: Over the past couple of years, most breaches, including credential harvesting have been the result of a successful phishing attack. Consider a site advisor for content filtering and review the security of your email servers.

- **Consider use of a site advisor "proxy", which includes web content filtering?**
  For instance, see document at this secure McAfee shortened URL - http://mcaf.ee/e9txw

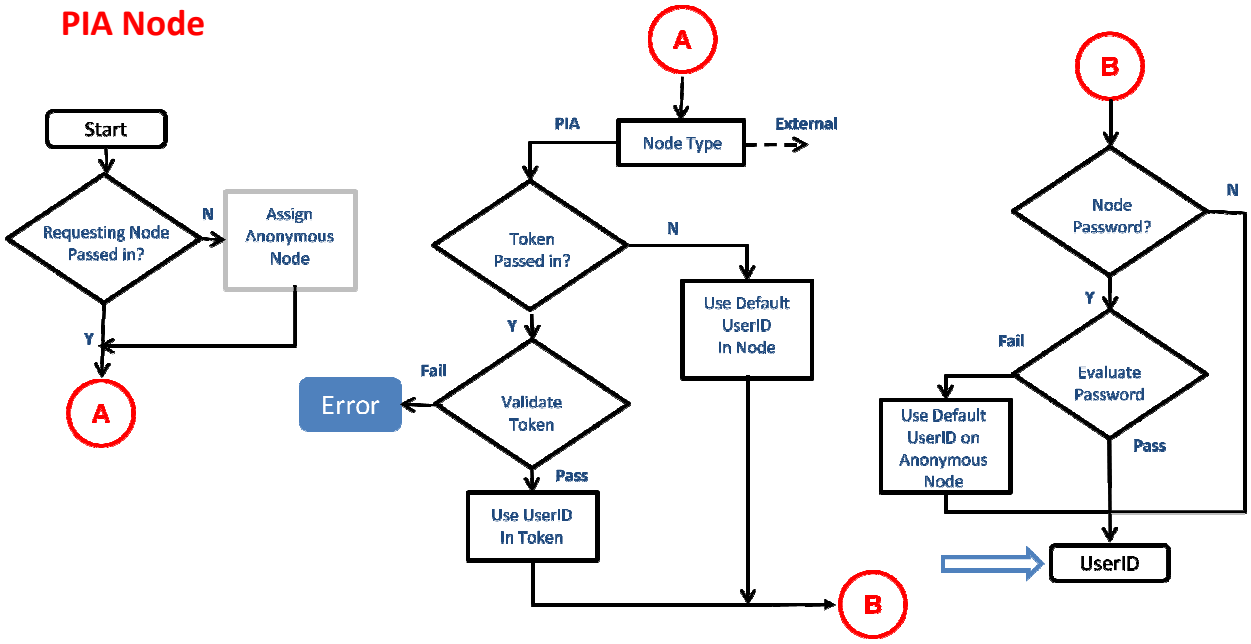
- **Check your exposure to phishing?**
  https://www.phishingscorecard.com/

All Security relies on Process, People and Technology

Implementing security from the inside out in a PeopleSoft environment

System hardening with reference to the additional concern for insider threat

- **Understand "Waterfall" User ID Flow in Integration Broker**
  If access drops through validation, access will use Roles of the **Default User** on the Anonymous Node, so you must ensure this user has minimal rights



==========