Chad Ballay

CIS411-342N Assessments and Audits (2207-DD)

Week 3 Written Assignment

5/9/2020

*2.1 Do not use vendor-supplied defaults for system passwords and other security parameters* (PCI Security Standards Council, n.d.)

Parsing this statement

**Do not use vendor supplied** – Either disable, remove, or otherwise neutralize unless reviewed and explicitly approved within the guidelines of your own security process. The vendor supplied seems to be arbitrary since any default password is a weakening of the security. The system parameters to a lesser degree. (HOW TO COMPLY TO REQUIREMENT 2 OF PCI , n.d.)

**Default System Passwords** – External entities are outside of your control so trusting them to maintain security around the passwords given with the apparatuses they supply is a future security vulnerability.

**Default Security Parameters** – External chosen parameters have no guarantee of aligning within your own security guidelines. Each parameter should be reviewed for how it fits within the overall security procedures and only then decided upon. For example, Websphere comes with several default admin accounts. A best practice is to instead generate new admin accounts unique to your own company’s needs. (WebSphere Commerce on premise not applicable for Commerce on Cloud offering, n.d.)

The assessment approach I would take would be in layers:

1. Awareness
   1. Review that written policies exist that communicate this requirement. This communication could be part of a collection of policies but there should be one specific policy covering this.
   2. Review that these policies have been communicated and will continue to be communicated to all employees that fall under scope for PCI-DSS. Ongoing training and communication mechanism will need to have delivery and acceptance auditability.
   3. Review that employees have audited and tracked communication mechanisms for communicating non-compliance or other concerns about adherence. An escalation pathway must be created that communicates to stakeholders their next steps in discharging their responsibility once they are aware of a compliance deficiency.
2. Implementation
   1. Teams/individuals would need to attest and show proof of instances of implementing this policy. Project plans, guidelines, checklist, customization scripts…. These items are to demonstrate proficiency and cultural awareness of how to do this. Ideally every system onboarded into the environment would have documentation of the standard setup and hardening process.
   2. Teams/individuals would need to show their own auditing process to ensure the process is being checked. Internal checks that teams have done themselves would need to be demonstrated to show that they are implementing redundancy in adherence to the policies.
3. Validation
   1. A subset up to including all items shall be periodically scanned for default accounts/passwords/settings. This scan would be carried out by members not directly aligned with the operations/administration role holders so as to ensure the reduction of conflict of interests.
   2. A subset of existing devices are to be replaced and validated once done that they meet compliance. This can be taken from the items replaced during the normal course of business.

The end result will be that no one should be unaware or able to say they didn’t have the chance to be made aware of this requirement. No operations/administration people should be able to say that they didn’t have the tools or policies as part their job duties to perform the needed actions. A separate set of people in the environment are responsible for helping ensure that the process is executed and that the items in question conform. Finally, if anyone has questions or concerns, they are aware of the next steps to perform to bring those details up.

# Works Cited

(n.d.). Retrieved from PCI Security Standards Council: https://www.pcisecuritystandards.org/

*HOW TO COMPLY TO REQUIREMENT 2 OF PCI* . (n.d.). Retrieved from PCI DSS Compliance: http://pcidsscompliance.net/pci-dss-requirements/how-to-comply-to-requirement-2-of-pci-dss/

*WebSphere Commerce on premise not applicable for Commerce on Cloud offering*. (n.d.). Retrieved from HCL: https://help.hcltechsw.com/commerce/7.0.0/com.ibm.commerce.pci.doc/concepts/csepcireq2.html