October 4, 2013

AD-Assurance Notes from October 4

Brian Arkills, UW
Michael Brogan, UW
Jeff Capehart, UFL
Eric Goodman, UCOP
Ron Thielen, U Chicago
David Walker, Internet2/InCommon
Ann West, Internet2/InCommon

Next Call

October 11 at Noon ET
+1-734-615-7474 PREFERRED
+1-866-411-0013

0195240#

Agenda:

- Review of comments received to date on the 2013 Cookbook
- Review of latest response from Microsoft

Notes

- Action Items
  - Brian will draft a response to Joe St Sauver's comments for review within our group before distribution on the Assurance list.
- The only comments received to date were from Joe St Sauver.
  - 4.1.2: We will clarify that we interpret IAP section 4.2.3.4 to apply only "...theft of the disk from a quiescent system," as Joe says. Other risks are addressed by other sections of the IAP.
    - We also continue to believe that sector-based decryption is an appropriate approximation of decrypting individual passwords. It was observed that many IdMS user records are actually larger than sectors.
  - 5.1.2: We will clarify that we're talking only about NTLMv1.
  - 5.3.4: We will remove the word "temporarily" and clarify that we expect the usual precautions taken when compromised accounts are discovered, not just changing the password.
  - 6: Ann has fixed the access restrictions.
  - 7.3: We'll remove the "need to validate algorithm" comments and explain why 72 hours.
  - 7.4: This is a valid management statement; the requirement in 4.2.3.6.3 is only that policies and procedures exist. We will clarify this in the interpretation of 4.2.3.6.3.
  - 7.6: Protected Channels *resist* eavesdropper attacks, which is the requirement, not to *preclude* eavesdropper attacks.
- Review of latest response from Microsoft
  - Microsoft observed, as did Joe, that storage encryption only mitigates risks associated with gaining physical access to disks. This is correct, but they use this as an argument that SysKey encryption is good enough, and we do not agree this meets the IAP requirement. They say that SysKey's algorithm is not published; we assume, therefore, that it is not approved.
  - We didn't finish our discussion, due to time constraints. We will continue next week.