AD Policy Working Group
Dec 19th, 2014
3110 Engineering Building II
3pm-4:30pm

Voting Members: Donna Barrett, Charles Cline, Dan Green, Julie Tilley, ~~Dan Evans~~, Daniel Henninger, Tom Farwig, ~~Joshua Gira~~, Payman Damghani

Ex Officio Members: Jeremy Brown, ~~Michael Underwood, Gene Morse, Jonn Perry~~

Guests: Billy Beaudoin, Debbie Carraway

Business handled outside of meetings:

NCSU-Read Group Memberships & userAccountControl attribute [B. Beaudoin, 11/5/14]
The userAccountControl attribute is the mask that shows if an account is disabled or locked out. I'd like to get that added to the list of attributes the NCSU-Read Group Memberships group can read. That way service accounts have the possibility of checking the account state before a login failing for either being disabled or being locked out.

ACTION: Committee Approved 11/6/14. Request awaiting AD Technical group approval.

=====

Agenda:

Push "InCommon RSA Server CA" to AD domain computers (D. Ballard)
I want to push the intermediary certificate authority "InCommon RSA Server CA" to domain computers. This intermediary cert is a subordinate cert of the "USERTrust RSA Certification Authority", which is already trusted by both Windows & all current, common web browsers.

S & C have been issuing host certs from the InCommon subordinate for some time. Most web servers include the InCommon subordinate as well as the actual host cert in TLS(/SSL) protocol negotiations, so it's not generally a problem in most cases. A corner case has been reported with InCommon certs on the VMware infrastructure where its not working like this, and certificate errors are being generated. Adding this intermediary cert to the Windows certificate store would resolve this particular corner case, and any other uses of the InCommon certs where it is not possible to bundle the intermediary cert with the host cert during TLS negotiations.

It's not clear that the AD Policy needs to approve, since we already trust the root cert, and InCommon host certs are already heavily used on campus, but just checking with you for good measure.

ACTION: Zero impact on security, but will help w/ certain apps that don't play well with Certificate. Committee Approved.

Followup on SSL v3 flaw / Poodle Exploit [D. Green / B. Beaudoin]
Should be noted that Derek released the "[OU]-EX-Microsoft-Disable SSLv3-0.0" group policy to campus to allow us to start easily disabling SSL -- it disables SSL (all versions) and explicitly enables TLS protocols, and disables SSL protocols in Internet Explorer (IE) 8.0 and above.

Everyone should begin testing with this and report issues. Our goal should be to move as many machines to this as we can.

After we're done with SSLv3, Billy suggests that we start turning off some of the ciphers that are bad. Here's a list of some that are being recommended to be killed by a number of sites:

- DES 56/56
- RC2 40/128
- RC2 56/128
- RC2 128/128
- RC4 40/128
- RC4 56/128
- RC4 64/128

Compiled from various Poodle remediation sites. Recommendation is to not allow the clients to keep defaulting down to these ciphers.

ACTION: Committee Approves and asks that AD Tech review the list of ciphers and implement a method to address this.

Proposal to Change Patching Schedule [G. Morse]
The SCCM Patching Service team would like to propose a change in the patching schedule. The current schedule is as follows:

- Early - Deployed on "Patch Tuesday"
- Normal - Deployed on Thursday following "Patch Tuesday"
- Late - Deployed on Tuesday following "Patch Tuesday"

The proposed changes would be:

- Early - Deployed on “Patch Tuesday”
- Normal - Deployed on Tuesday following “Patch Tuesday”
- Late - Deployed on 2nd Thursday following “Patch Tuesday”

These changes would give people in the early group more time to test patches. If Microsoft announces bad patches, it allows the patching team to not approve those patches for normal and late groups.

Discussion: Pushing the Normal to after the weekend will cause significant delays for folks that reboot their machines over the weekend. So rather than adding 4 days, you’re actually adding 9 days.

ECE notes that we tend to have a few machines that don’t come up happy after each month -- so we’d like to have it not occur on a Friday (one suggestion was to push it back a day) so we have a working day to fix these and not have them down for the entire weekend.

Payman has concerns about delaying critical patches.

We could move Late from the Tuesday to the Thursday if that would be helpful?

COM, CHASS, ENGR don’t feel that there’s been enough of a negative impact to change the current schedule.

Recommend that groups with any servers in Normal be moved to Late to lessen the chance that a revoke would impact services. Also, they should consider not allowing auto reboot of machines when patching.

Plus they could change their client to not check for updates on certain days (or use maintenance windows if using SCCM patches) to better control when they patch or *react* to release patches.

ACTION: Committee Rejects and recommends that folks review alternatives above.

Adding ADMX files for Direct Access to Central Store [M. Underwood]
Michael has provided us with the ADMX files needed for Direct Access management / group policies to be available in the WolfTech domain. Have already been tested in the WolfTest domain. Request is to add to the domain so beta testing of DA service can begin.

ACTION: Committee Approves and will direct DC Admins to implement.

Followup on Requiring SANS Securing the Human Videos for OU Admins (B. Beaudoin)

The SCGS has discussed trying to get a subset of these videos required for all staff, but it will be quite a while. Therefor they are looking for groups to opt-in to requiring them. There are around 50 3-10 minute videos, so clearly not all of them would need to be required, just a subset that the committee agrees upon.

https://moodle-projects.wolfware.ncsu.edu/course/view.php?id=789

The committee was asked to review these videos prior to this meeting.

Henninger: “In general I think the videos are good. They are certainly a little "silly" at times and a lot of the stuff you find yourself going "... I know all this..." BUT I think it serves as a good reminder of the types of things your users might think/go through. I did actually learn something about FERPA that I didn't know when I got to that video so that was cool. --- so I would say they are worth it to make sure you are aware of the basics, and also to "remind you" of things you probably take for granted.”

How do we DO this? Ask and hope that most do it?
Start of a professional development program? (let’s start simple, but yes, could lead to that)
Can we gamify it? Needs better implementation / infrastructure -- need to record/reward.

ACTION: Billy go talk to DELTA about getting another course setup similar to the one linked above.

Followup from Charles re: ADFS/Azure [C. Cline]

Update on the rollout of the ADFS/Azure infrastructure required for the campus Office365 implementation. ADFS functional, synchronization in place (WolfTech to Azure AD). Testing continues (TSS leading) with about 50 accounts; this is usage testing -- but the accounts are production. Even once synch’d, accounts must still be provisioned for Office365.

In Jan, TSS plans to open “Phase2” rollout of IT folks across campus. Ahead of general campus rollout.

We’re matching the same attributes as we do with Shib service. Sync also limited to the People OU -- fname, lname, unityID, email.

Followup on PCI & WolfTech AD [B. Beaudoin / D. Carraway]

Update on the state of the compliance efforts/discussions. Based on further information/clarifications provided from the QSA and on discoveries that we made about our campus environment, we’re re-examining the idea of keeping PCI within Wolftech AD rather than splitting off into another domain as had previously been decided.