"Monitor and Mitigate" Alternate Control for Satisfying Requirement 4.2.3.6.3 in Active Directory Domain Services Environments - DRAFT 2013102

"Monitor and Mitigate" Alternate Control for Satisfying Requirement 4.2.3.6.3 in Active Directory Domain Services Environments

Scope

Requirement 4.2.3.6.3 addresses certain risks which may arise when credentials are transmitted over networks in an insecure manner. While it may be possible to avoid this risk through appropriate client workstation configuration, common configurations of Active Directory Domain Services may expose AD users' credentials in this way, due to non-conforming client configurations.

Intent

Provide a process by which credentials exposed to possible compromise through the use of unsigned, i.e. unencrypted, BINDs or the use of NTLMv1 are identified and become ineligible for Silver assertions within 72 hours of such use.

Risks

In Active Directory Domain Services environments where the domain controllers have not yet or will not be configured in a way to prevent the use of unsigned LDAP BINDs and Windows network authentication based on either LANMAN or NTLMv1 protocols, user credentials may be transmitted either in the clear or through provably insecure authentication protocols.

The risk is mitigated by an automated audit process which identifies all such users and in cases where the users have been vetted for Silver assertions and revokes their eligibility for Silver within 72 hours. The client side cause will then have to be identified and resolved, at which point the user may recertify their credentials using whatever approved process the IdPO has established for such. In the event that the end user recertifies their credentials without resolving the client-side issue or a different issue arises, the credentials will be invalidated by the next failing audit.

Assertion

For requirement 4.2.3.6.3, the process of auditing the use of unsigned BINDs and non-NTLMv2 authentication used with the Active Directory Domain Services environment exceeds the requirements in that it assumes that any user's credentials exposed on the network have been compromised regardless of any other evidence in support or contradiction of that.

Discussion

There are many cases where the IAP establishes requirements that can be circumvented by end-users. For example, the IAP contains many requirements for the protection of passwords that can be circumvented by an end-user posting their password on a bulletin board. The IAP acknowledges this example in 4.2.4.2.1: "The IdPO shall revoke Credential s within 72 hours after being notified that a Credential is no longer valid or is compromised." IdPOs also mitigate this risk through policy and education.

There are other IAP requirements for which non-compliance by an end-user does not necessarily result in credential compromise, but should result in the loss of eligibility for one or more assurance profiles. This is particularly true when compliance relies on the use of end-user devices that meet specific technical requirements for supported platforms, software revisions, malware mitigation, *etc*. Further, it is often impractical for an IdPO to completely prevent non-compliance by end-users when compliance is required only for a subset of the IdPO's community. In fact, business requirements for the use of specific technology tools may force non-compliance for some other subset of the community. 4.2.3.6.3 is an example of such IAP requirements.