searchWin2000.comManageability

March 13, 2002 *a newsletter from TechTarget*

Windows 2000 in the Enterprise: Technology strategies in action

Single forest vs. multi-forest Active Directory design

by Meredith B. Derby, assistant news editor

Anyone who has deployed Active Directory (AD) and set up a good AD management process deserves a breather. A short one, that is, because one of the toughest tasks in managing AD is just around the corner: security.

Any venture into AD security should involve multi-forest AD designs, said AD security expert Ratmir Timashev. The reason? In a Jan. 30 security bulletin, Microsoft revealed an Active Directory Domain Trust vulnerability. The bulletin stated that "trusting domains do not verify domain membership of SIDs in authorization data."

If you can't see the forest through the trees in AD security, never fear. In this SearchWindowsManageability (SWM) interview, Aelita Software CEO Ratmir Timashev explains how the number of forests relates to Active Directory's security. Powell, Ohio-based Aelita worked with Microsoft to identify the recent domain trust vulnerability.

SWM: How does Active Directory organize the elements of a network, such as users and computers?

Timashev: Active Directory has three key containers. A forest is a collection of domains and is the highest-level container for network objects. Domains are level-down containers within a forest and represent an administrative and replication boundary. Domains are normally created for geographical or organizational reasons. The main purpose is to separate administration and/or reduce replication. Organizational units (OUs), which can be departments or groups, are used to structure and manage your network in a way that reflects a company's business organization.

SWM: Can you define single forest vs. multi-forest Active Directory design?

Timashev: A single forest design is the simplest design. There is only one forest for the whole company network. In other words, all the network objects for the whole company are organized within a single forest. A single Active Directory forest design is easier to administer, provides lower support costs, and offers the best collaboration and messaging environment for the whole company. However, a single forest is the least secure design.

A multi-forest design is when the entire company's network is separated into several forests. It carries higher administrative and support costs, and complicates collaboration and messaging. However, it provides the highest level of security.

SWM: How does the number of forests relate to security, particularly the Domain Trust vulnerability in AD?

Timashev: A domain used to be considered a security boundary. A domain as a security

boundary holds users, computers, and other account information; provides security authentication; and controls access to the resources within the domain. A domain in Windows 2000 Active Directory cannot be considered a security boundary because of the following: Domains have automatic transitive trust relationships within a forest; all domain controllers have a writable copy of a security database; there is a writable copy of a Global Catalog available on domain controllers in all domains in the forest; the "Domain Trust" vulnerability and security identification (SID) history mechanism.

A domain in Windows 2000 is no longer a security boundary, and it does not provide enough security isolation. A rogue administrator in one domain can potentially get unauthorized access to resources in all domains in the forest by using the "Domain Trust" vulnerability or manipulating the Global Catalog. So, a single forest with multiple domains means no security boundaries in the directory.

SWM: How exactly does multi-forest design benefit an organization?

Timashev: By default, a user or administrator in one forest cannot access another forest, which means that the forest is a security boundary. A multi-forest design allows for security boundaries within corporate networks, thus improving the overall network security. The most sensitive parts of the network (corporate, accounting, finance, R&D, etc.) should be in a separate forest to guarantee the highest level of security and access control. In addition, different divisions within a large corporation should consider a separate forest for added security isolation.

Of course, some users might need to access data in another forest. For this need, administrators can create trust relationships between domains in the forests and use SID filtering, which is a mechanism that prevents the "Domain Trust" vulnerability from occurring between forests.

SWM: Can SID filtering be used between domains within the same forest to prevent the Domain Trust vulnerability?

Timashev: Unfortunately no. SID filtering cannot be used between domains in the same forest because it would prevent Active Directory from functioning properly.

SWM: What kinds of companies should consider a multi-forest design?

Timashev: Companies that might consider multi-forest designs are medium to large sized. They have more administrators, which increases the risk of having less supervision and the possibility of a rogue admin. Multi-forest designs will be most useful to financial, banking, insurance, healthcare and government services organizations. Of course, some of these fields are required by law or business practices to implement high levels of security.

SWM: Are there any drawbacks to multi-forest designs?

Timashev: Administrators need to consider how data might need to be synchronized between the forests and what administration practices and tools might be needed. The most important issue, though, is how to set up Exchange on a multi-forest network. Generally, administrators will need to implement either one Exchange organization for the entire network or have separate Exchange organizations for each forest.

allow 24 hours for your "REMOVE" request to be processed.