Best Practices in LDAP Security

by Andrew Findlay

LDAP servers are part of the critical infrastructure of most large organisations. They hold personal data subject to legal protection, and often act as the authoritative source of authentication and authorisation for multiple applications.

This paper divides LDAP security into three major requirements: availability, data integrity, and data confidentiality. Appropriate controls are proposed for each topic, noting the interactions and compromises that are required. Most of the controls are technical, relating to design and administration issues that affect all LDAP server products. The trade-off between technical and organisational controls is discussed, with reference to common human-factors issues.

Availability is defined in the SANS security glossary as "the need to ensure that the business purpose of the system can be met and that it is accessible to those who need to use it". Technical measures to meet this requirement include replication, load-balancing and load-limiting, proxy servers and caches, server tuning and OS tuning. Management controls include planning for no-break upgrades, co-ordination of server configuration with network configuration, backup procedures, and change-control procedures.

Data Integrity controls must ensure that data is protected from unauthorised modification. The key technical measures are the use of access-control rules and appropriate forms of authentication.

Confidentiality includes protecting the entire service from access by unauthorised users, preventing the exposure of sensitive data, and protection of data both at rest on disk and in transit across the network. The controls include further access-control, data encryption and session encryption, the use of read-only subset replicas, and appropriate DIT design to avoid exposure of sensitive data in DNs.

It is intended that this paper should spark a discussion of best practices among LDAP practitioners, leading to a consensus document which can be submitted for publication as a SANS SCORE checklist.