The Top-50 Active Directory Delegated Administrative Access Reports

Paramount Defenses recommends that all organizations that operate on Active Directory (AD) accurately* identify and lockdown the number of individuals who possess delegated administrative access domain-wide in Active Directory.

The following 50 AD delegated administrative access audit reports can help organizations fulfill this cyber security need –

DOMAIN USER ACCOUNT MANAGEMENT

1. Who can create user accounts in Active Directory?
2. Who can delete user accounts in Active Directory?
3. Who can reset the passwords of user accounts in Active Directory?
4. Who can disable/enable user accounts in Active Directory?
5. Who can unlock locked user accounts in Active Directory?
6. Who can change the logon name of user accounts in Active Directory?
7. Who can change the logon hours for user accounts in Active Directory?
8. Who can change the logon script for user accounts in Active Directory?
9. Who can change the profile path of user accounts in Active Directory?
10. Who can change the expiration date of user accounts in Active Directory?
11. Who can disable/enable the use of Smartcards for interactive logon for user accounts in Active Directory?
12. Who can change the setting "*account is sensitive and cannot be delegated*" on user accounts in Active Directory?
13. Who can change whether or not Kerberos pre-authentication is required for user accounts in Active Directory?
14. Who can change whether or not DES encryption types should be used for user accounts in Active Directory?
15. Who can change the security permissions protecting user accounts in Active Directory?

II. DOMAIN COMPUTER ACCOUNT MANAGEMENT

16. Who can create computer accounts in Active Directory?
17. Who can delete computer accounts in Active Directory?
18. Who can change the computer name (Pre-Windows 2000) of computer accounts in Active Directory?
19. Who can change the DNS name of computer accounts in Active Directory?
20. Who can change the machine role of computer accounts in Active Directory?
21. Who can change the Service Principal Names (SPNs) of computer accounts in Active Directory?
22. Who can change the security permissions protecting computer accounts in Active Directory?

For domain computer accounts, one may also wish to determine who can change various Kerberos delegation settings on these accounts.

III. DOMAIN SECURITY GROUP MANAGEMENT

23. Who can create security groups in Active Directory?
24. Who can delete security groups in Active Directory?
25. Who can change the membership of security groups in Active Directory?
26. Who can change the scope of security group in Active Directory?
27. Who can change the type of security group in Active Directory?
28. Who can change the name (Pre-Windows 2000) of security groups in Active Directory?

29. Who can change the description of security groups in Active Directory?
30. Who can change the email-address of security groups in Active Directory?
31. Who can change the security permissions protecting security groups in Active Directory?

IV. ORGANIZATIONAL UNIT (OU) MANAGEMENT

32. Who can create organizational units in Active Directory?
33. Who can delete organizational units in Active Directory?
34. Who can disable group policies linked to organizational units in Active Directory?
35. Who can change the list of group policies linked to organizational units in Active Directory in Active Directory?
36. Who can change the precedence of group policies linked to organizational units in Active Directory?
37. Who can change the security permissions protecting organizational units in Active Directory?

V. SERVICE CONNECTION POINT MANAGEMENT

38. Who can create service connection points in Active Directory?
39. Who can delete service connection points in Active Directory?
40. Who can change the keywords of service connection points in Active Directory?
41. Who can change the service DNS name of service connection points in Active Directory?
42. Who can change the security permissions protecting service connection points in Active Directory?

VI. GROUP POLICY MANAGEMENT

43. Who can create group policy containers in Active Directory?
44. Who can delete group policy containers in Active Directory?
45. Who can change the security permissions protecting group policy containers in Active Directory?

VII. PUBLISHED PRINTER MANAGEMENT

46. Who can create (publish) printers in Active Directory?
47. Who can delete published printers in Active Directory?
48. Who can change the share name of published printers in Active Directory?
49. Who can change the security permissions protecting published printers in Active Directory?

VIII. DOMAIN SECURITY MANAGEMENT

50. Who can change the security permissions protecting the domain root in Active Directory?

* For reports 15, 22, 31, 37, 42, 45, 49 and 50, above, additionally one may also wish to consider who can change the ownership of these objects.

***** The accurate identification of who has what privileged access in Active Directory requires the precise determination of exactly who has what Active Directory Effective Permissions on various pertinent objects inside Active Directory.