CHECK

connecT
SYSTEMHAUS AG

20 MAßNAHMEN
ZUR ABSICHERUNG IHRES ACTIVE DIRECTORY

erledigt

1 Richten Sie Microsoft LAPS zur Passwortverwaltung lokaler Admin-Konten ein.

2 Teilen Sie Berechtigungen zur Administration in Tiering-Level auf.

3 Schützen Sie Domänen-Administratoren und privilegierte Domänen-Konten, indem Sie:

- 3A Die Anmeldung an Clients verhindern
- 3B Die Anmeldung als Dienst verhindern
- 3C Die Anmeldung als Batch-Job verhindern
- 3D Die Nutzung solcher Konten in Diensten und Anwendungen unterbinden

4 Setzen Sie Berechtigungen und Strukturen in Rollen/Gruppen um.

5 Vergeben Sie keine Berechtigungen für „Domänen-Benutzer“ oder allgemeine Standard-Gruppen/Konten.

6 Beschränken Sie die Internetverbindung/ Browser-Sessions für privilegierte Konten.

7 Verhindern Sie, dass RDP Verbindungen mit privilegierten Konten über Client-Workstations hergestellt werden können.

8 Erneuern Sie regelmäßig das Passwort des „Kerberos Distribution Center (KDC)“ Dienstkontos.

9 Segmentieren Sie Tier-0 und Tier-1 Systeme auf Netzwerkebene.

10 Richten Sie starke Passwortrichtlinien für Benutzer und Administratoren ein.

11 Nutzen Sie spezielle Workstations oder Jumphosts für die Administration des Active Directory.

SEITE ZURÜCKSETZEN

DOKUMENT SPEICHERN

Bei den o.g. Punkten ist die Umsetzung selbstverständlich individuell zu prüfen. Änderungen müssen kontrolliert und bewusst geplant und umgesetzt werden.

connecT
SYSTEMHAUS AG

20 MAßNAHMEN
ZUR ABSICHERUNG IHRES ACTIVE DIRECTORY

12 Nutzen Sie Managed/Group-Managed Service Accounts für Dienste und Applikationen.

13 Der AD-Controller bleibt AD-Controller: Der Funktionsumfang bleibt maximal reduziert. DHCP und Applikationen haben hier nichts verloren.

14 Spooler-Dienst im Serverumfeld: Stellen Sie sicher, dass der Spoolerdienst ausschließlich auf erforderlichen Servern aktiviert ist.

15 Sorgen Sie für eine sichere Konfiguration des DNS: Die Default-Konfiguration reicht nicht aus.

16 Stellen Sie sicher, dass Domänen-Benutzer keinerlei administrativen Rechte besitzen.

17 Deaktivieren Sie Netbios und LLMNR.

18 Überprüfen Sie das Active Directory regelmäßig mit professionellen Tools auf Schwachstellen. Dadurch haben Sie die Möglichkeit, stets auf neueste Indikatoren und Prüfroutinen zurückzugreifen.

19 Überprüfen und Überwachen Sie dauerhaft auf Anomalien:

- 19A Gruppenrichtlinien
- 19B Privilegierte und sensible Konten/ Gruppen

20 Stellen Sie sicher, dass das Active Directory zusätzlich zum vorhandenen Backup, konsistent und unabhängig vom Betriebssystemen gesichert wird.

SEITE ZURÜCKSETZEN

DOKUMENT SPEICHERN

Bei den o.g. Punkten ist die Umsetzung selbstverständlich individuell zu prüfen. Änderungen müssen kontrolliert und bewusst geplant und umgesetzt werden.