How to Protect Your Active Directory from Attacks

10 Key Areas to Focus On

1 PRIVILEGED USERS AND GROUPS

- [ ] Review / minimize privileged group membership
- [ ] Remove admin permissions granted to service accounts
- [ ] Monitor for permission changes on the AdminSDHolder object

2 PRIVILEGED ACCESS HARDENING

- [ ] Review / use separate named admin accounts
- [ ] Review / create break glass accounts
- [ ] Deploy a tiered administrative model
- [ ] Enable just-in-time access
- [ ] Use Privileged Access Workstations

3 MONITOR FOR UNUSUAL ACTIVITY

- [ ] Implement a SIEM with UEBA capabilities
- [ ] Monitor privileged groups for membership changes
- [ ] Review / watch for ACL changes on sensitive objects

4 IDENTITY MANAGEMENT

- [ ] Remove inactive users
- [ ] Review sensitive data / application access
- [ ] Update service account passwords

5 DOMAIN CONTROLLER HARDENING

- [ ] Review / remove unnecessary server roles and agents
- [ ] Review / disable the Print Spooler service on all domain controllers

6 DETER LATERAL MOVEMENT

- [ ] Implement LAPS on all member servers and client computers
- [ ] Review / restrict local admin group membership

7 TRUST SECURITY

- [ ] Ensure SID filtering is active
- [ ] Enable Selective Authentication where possible

8 BACKUP AND RECOVERY

- [ ] Backup at least two domain controllers in every domain
- [ ] Test backups regularly
- [ ] Isolate backups to keep them free of malware
- [ ] Use an AD-aware backup and recovery tool

9 KERBEROS MANAGEMENT

- [ ] Rotate the KRBTGT password annually
- [ ] Remove SPNs assigned to privileged accounts
- [ ] Eliminate unconstrained delegation
- [ ] Block delegation to privileged accounts

10 SECURE YOUR DEPENDENCIES

- [ ] Review / limit hypervisor admin privileges
- [ ] Review / restrict access to storage that contains copies of the DIT
- [ ] Review / evaluate PAM tool permissions

+1 844 267 0804
info@ravenswoodtechnology.com
ravenswoodtechnology.com

RAVENSWOOD TECHNOLOGY GROUP