Active Directory Audit

Active Directory Audit: Hvorfor er det vigtigt?

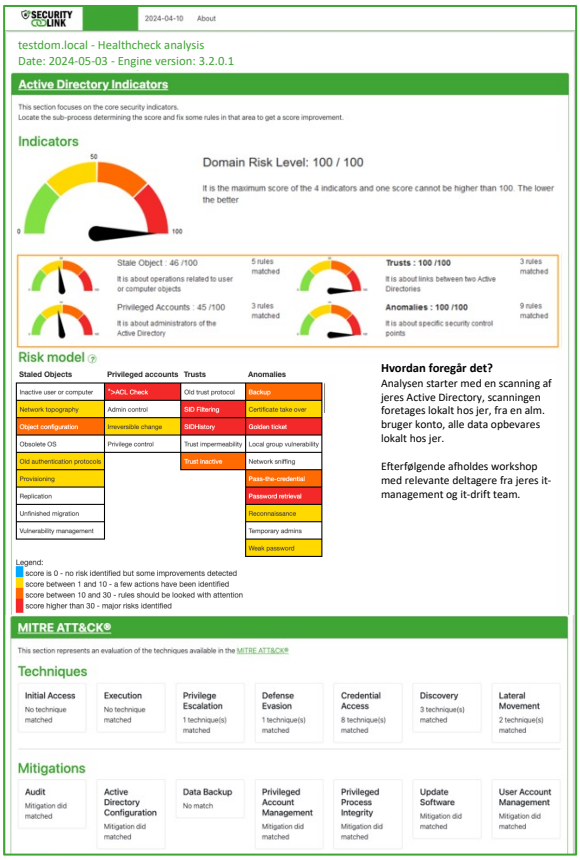
Active Directory er en vital del af jeres IT-infrastruktur, men også et udsat angrebsmål. Hackere kan udnytte svagheder i jeres Active Directory til at få adgang til jeres ressourcer, data og applikationer.

Derfor bør I lave et Active Directory Audit regelmæssigt. Det er en systematisk gennemgang af jeres Active Directory miljø, der hjælper med at:

- Få et overblik over eventuelle trusler, der ligger gemt i Active Directory, såsom malware, ransomware, phishing, 'privilege escalation', 'lateral movement', etc.
- Identificere og deaktivere konti uden password-udløb, administrative konti, bruger- og computerkonti, der ikke bliver brugt. Disse konti kan være en sikkerhedsrisiko, hvis de bliver misbrugt eller udnyttet.
- Forbedre og optimere Active Directory konfigurationen, rettighederne, politikkerne, objekterne, backuppen, osv. Disse aspekter kan påvirke Active Directory's funktionalitet, stabilitet og sikkerhed.

Et Active Directory Audit kan give en værdifuld indsigt i jeres Active Directory miljø, samt anbefalinger til, hvordan I kan forbedre det. Det kan også hjælpe med at overholde lov og compliancemæssige krav, såsom NIS2, GDPR, ISO 27001 m.v..

Hvis I vil have udført et Active Directory Audit, eller hvis I har spørgsmål om emnet, så kontakt SecurityLink. Vi har mange års erfaring med Active Directory, og kan tilbyde en professionel og skræddersyet service, der passer til jeres behov.



Resultaterne opsummeres i et Executive Summary, og der er grundige tekniske vejledninger til forklaring og mitigering af de fundne sårbarheder.

Kontakt os:
securitylink.dk
info@securitylink.dk

Active Directory Audit

Hvordan gør vi det?

1. **Opstartsmøde**
   Indledende dialog, hvor vi diskuterer jeres organisations situation og mål, potentielle trusler og prioriterede risici. Vi aftaler tidsplan og bestemmer yderligere detaljer.

2. **Informationsindsamling**
   SecurityLink får adgang til jeres miljø i en aftalt periode.

3. **Informationsanalyse**
   De indsamlede oplysninger analyseres imod kendte sårbarheder og 'best practices' fra bl.a. Microsoft, ANSSI, MITRE ATT&CK®.

4. **Oprettelse af rapportering**
   De indsamlede informationer samles i en rapport, som inkluderer et resumé samt alle resultater og anbefalinger på de forskellige områder.

5. **Præsentation**
   Der afholdes workshop med en mundtlig præsentation af rapporten, som også vil indeholde en dialog om håndtering af identificerede problemstillinger. Dermed får I øget jeres viden igennem indsigt og sparring med vores specialister og et kickstart til det næste trin – udarbejdelse af en køreplan baseret på resultaterne.

I får bl.a. jeres sårbarheder vist i forhold til relevante områder i MITRE ATT&CK® frameworket.

Tag en dialog med en af SecurityLinks specialister, sammen begynder vi rejsen for at beskytte din organisations følsomme oplysninger.

Kontakt os:
securitylink.dk
info@securitylink.dk