Mandatory Integrity Control (MIC)

auch: Windows Integrity Control (WIC)

Grundprinzip: No Write up-Policy

Ein Subjekt mit niedrigerem Integritätslevel
kann nicht
auf ein Objekt mit höherem Integritätslevel
schreibend zugreifen.

Integritätslevel

Deutsch	Englisch	SID	Hex	SDDL	Bsp. Subjekt	Bsp. Objekt
Nicht vertrauenswürdige Verbindlichkeitsstufe	**Untrusted** Mandatory Level	**S-1-16-0**	**0**	**-**		
Niedrige Verbindlichkeitsstufe	**Low** Mandatory Level	**S-1-16-4096**	**1000**	**LW**	IE Protected Mode	%userprofile%\ |-AppData\ |-**LocalLow** |-Local\ |-Temp\ |-**Low**
Mittlere Verbindlichkeitsstufe	**Medium** Mandatory Level	**S-1-16-8192**	**2000**	**ME**	Benutzer	„normale“ Datei
Mittlere gehobene Verbindlichkeitsstufe	Medium Plus Mandatory Level	S-1-16-8448	2100			
Hohe Verbindlichkeitsstufe	**High** Mandatory Level	**S-1-16-12288**	**3000**	**HI**	Administratoren	
System-verbindlichkeitsstufe	**System** Mandatory Level	**S-1-16-16348**	**4000**	**SI**	SYSTEM	
Verbindlichkeitsstufe für geschützte Prozesse	Protected Process Mandatory Level	S-1-16-20480	5000			
Verbindlichkeitsstufe für sichere Prozesse	Secure Process Mandatory Level	S-1-16-28672	7000			

Subjekt (wer greift zu)

Subjekt	Integritätslevel	Anzeige des Integritätslevels
Benutzer	Eintrag im Access-Token	**whoami /groups**
Prozess	geerbt vom aufrufenden Prozess, bzw. Benutzer	**ProcessExplorer**

Objekt (auf wen wird zugegriffen)

Alle Securable Objects,
z.B. **Ordner**, **Dateien**, **Registry-Keys**, **Dienste**, **Drucker**, **Prozesse**, **Benutzer**, **Gruppen**, **Computer**.

Objekt	Integritätslevel	Anzeige des Integritätslevels
Ordner, Datei	Eintrag in der SACL, bzw. kein Eintrag => Medium	**icacls** *Datei*, **chml.exe**
Prozess	geerbt vom aufrufenden Prozess, bzw. Benutzer	**ProcessExplorer**
sonstige	Eintrag in der SACL, bzw. kein Eintrag => Medium	-