## Vorgehen bei InstallShield-Problemen:

- 1. Nicht ausreichende Berechtigungen Zur Installation werden administrative Rechte benötigt
- 2. Wenn gerade ein InstallShield-Setup gelaufen ist, benötigt die Installations-Engine einige Sekunden, um die Installation sauber zu beenden. In dieser Zeit läuft eine von einem vorherigen Prozess gestartete Instanz von Ikernel.exe im Speicher – daher lässt sich kein neues Setup starten. Nach einigen Sekunden sollte der Start wieder möglich sein.
- 3. Prüfen, ob keine Ikernel.exe-Instanz im Speicher läuft (Task-Manager). Falls ja, und es gibt kein laufendes Setup, den Prozess beenden.
- 4. Temp-Verzeichnis löschen. In der Regel ist es C:\Users\aktuellerNutzer\AppData\Local\Temp. Der aktuelle Speicherort findet sich auch in den Umgebungsvariablen TEMP und TMP (Systemsteuerung → System → Erweiterte Systemeinstellungen → Umgebungsvariable...). Evtl. muss die Ordner-Ansicht im Explorer angepasst werden (Versteckte Dateien anzeigen!)
- 5. Den Ordner C:\Programme\Common Files\InstallShield löschen und das Setup neu starten.

```
Bei 64-Bit-Version: C:\Programme (X86)\Common Files\InstallShield löschen und das Setup neu starten.
```

- 6. Die Neuinstallation des Internet Explorers und/oder der Windows Service Packs repariert etliche defekte/fehlende Systemdateien.
- 7. Ungenügende COM-Berechtigungen:
  - klicken Sie auf Start
  - geben Sie im Feld *Suche starten* dcomcnfg ein und bestätigen Sie mit der ENTER-Taste



- geben Sie Ihre Zustimmung, dass der Vorgang durchgeführt werden soll (evtl. müssen Sie Ihr Administratorpasswort eingeben)
- öffnen Sie Komponentendienste und Computer



- klicken Sie mit der rechten Maustaste auf Arbeitsplatz und wählen Sie Eigenschaften
- klicken Sie auf COM-Sicherheit

Allgemein	Optionen	Standardeigenschaft	en
Standardprotokoll	e COM-S	iicherheit MSD	TC
Zugriffsberechtigun	gen		
Sie können die E Anwendungen b Anwendungen s Warnur sich dar sicher V haben u Start- und Aktivieru Sie können die S Anwendungen u können Sie Limit	erechtigungen für de earbeiten. Zudem kör etzen, die ihre eigenen ig: Das Ändem von Z auf auswirken, ob An ferbindungen herstelle und/oder sicher ausge Limits bearbeiter ngsberechtigungen Standardberechtigung nd das Aktivieren von s für Anwendungen s	n Standardzugriff auf nnen Sie Limits für n Berechtigungen festleger ugriffsberechtigungen kanr wendungen sicher starten, n., sichere Funktionsweiser eführt werden können. Standard bearbeite en für das Starten von n Objekten bearbeiten. Zud etzen, die ihre eigenen	n n em
Perception page :	festlegen		
Wamur Aktivien Anwenc herstelle ausgefü	ig: Das Ändem von S ungsberechtigungen k dungen sicher starten, en, sichere Funktionsv ihrt werden können.	tart- und cann sich darauf auswirker sicher Verbindungen weisen haben und/oder sic	her
Warmun Aktivien Anwend herstelle ausgefü	ig: Das Ändem von S ungsberechtigungen i dungen sicher starten, en, sichere Funktionsw ihrt werden können.	tart- und cann sich darauf auswirker sicher Verbindungen weisen haben und/oder sic n) Standard bearbeiter	n, ol her
Veitere Informationer	ng: Das Ändern von S ungsberechtigungen H lungen sicher starten, en, sichere Funktionswicht ihrt werden können. Li <u>m</u> its bearbeiter n zum <u>Festlegen diese</u>	tart- und kann sich darauf auswirken sicher Verbindungen weisen haben und/oder sic n) Standard bearbeiter <u>ar Eigenschaften</u> .	n, ol her

- klicken Sie unter Zugriffsberechtigungen auf Standard bearbeiten...
- prüfen Sie, dass SYSTEM oder Sie als Nutzer Zugriffsberechtigung haben

ruppen- oder Benutzem	amen:		
SELBST			
SYSTEM			
		instruction CI	v
	(		(
	Hinzufü	gen	Entfernen
erechtigungen für SYST	EM		
erechtigungen für SYST	EM 2	Zulassen	Verweigem
erechtigungen für SYST Lokaler Zugriff	EM Z	Zulassen	Verweigem
erechtigungen für SYST Lokaler Zugriff Remotezugriff	EM Z	Zulassen	Verweigen
erechtigungen für SYST Lokaler Zugriff Remotezugriff	EM Z	Zulassen	Verweigen
erechtigungen für SYST Lokaler Zugriff Remotezugriff	EM 2	Zulassen	Verweiger
erechtigungen für SYST Lokaler Zugriff Remotezugriff	EM Z	Zulassen	Verweigem
erechtigungen für SYST Lokaler Zugriff Remotezugriff	EM 2	Zulassen	

- setzen Sie ggf. ein Häkchen bei Zulassen
- klicken Sie auf OK
- schliessen Sie die Komponentendieste und starten Sie die Installation neu.
- 8. Ein potentieller Fehler sind fehlende Dateien stdole32.tlb, stdole.tlb. Es handelt sich um Windows-eigene Dateien, die sich auf dem Rechner (C:\Windows\system32) befinden sollten. Beim Kopieren von einer anderen Maschine sicherstellen, dass die gleiche Windows-Version verwendet wird.
- 9. Prüfen Sie, dass die Standardidentitätswechselebene auf Identifizieren gesetzt ist:
  - klicken Sie auf Start
  - geben Sie im Feld *Suche starten* dcomcnfg ein und bestätigen Sie mit der ENTER-Taste



• geben Sie Ihre Zustimmung, dass der Vorgang durchgeführt werden soll (evtl. müssen Sie Ihr Administratorpasswort eingeben)



• öffnen Sie Komponentendienste und Computer

- klicken Sie mit der rechten Maustaste auf Arbeitsplatz und wählen Sie Eigenschaften
- klicken Sie auf Standardeigenschaften

and the second	e COM	-Sicherheit	MSDTC
Allgemein	Optionen	Standard	deigenschaften
COM-Internetdiens Standardeigenscha Die Authentifizierun Standardauthenti Verbinden	ste auf diesem Com ften der DCOM-Kor gsebene gibt die Si fizierungsebene:	puter aktivieren mmunikation cherheit auf Pak	etebene an.
)ie Identitätswechs rkennen und Vorg usführen können.	selebene gibt an, ot änge unter Verwen	o Anwendungen dung der Identitä	Aufrufer ät des Clients
Die Identitätswechs srkennen und Vorg susführen können. Standardidentität: Identifizieren	selebene gibt an, ot änge unter Verwen swechselebene:	Anwendungen dung der Identitä	Aufrufer ät des Clients
Die Identitätswechs erkennen und Vorg susführen können. Standardijdentität: Identifizieren Sicherheit für Verwy venn Authentifizien Standardidentitätsw <u>Z</u> usätzliche Si	selebene gibt an, ot änge unter Verwen swechselebene: eisprotokollierung k ung verwendet wird vechselebene nicht cherheit für Verwei	Anwendungen dung der Identitä 	Aufrufer ät des Clients t werden,

- unter Standardidentitätswechselebene muss Identifizieren ausgewählt sein
- klicken Sie auf Übernehmen und OK
- schliessen Sie die Komponentendienste
- 10. Eine weitere Problemursache können fehlende Rechte bei folgenden Registry-Schlüsseln sein:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\CLSID HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Interface HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\TypeLib

Zum Ändern regedit verwenden. Folgende Nutzer brauchen vollen Zugriff:

Administrator (der lokalen Maschine) System Ersteller-Besitzer

Vor dem Ändern der Registry ist es empfehlenswert, die zu ändernden Schlüssel zu exportieren.

11. Kontrollieren Sie mittels regedit im Schlüssel

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion den Wert CommonFilesDir. Der hier stehende Pfad darf keine führenden Leerzeichen oder Tabulatoren enthalten.