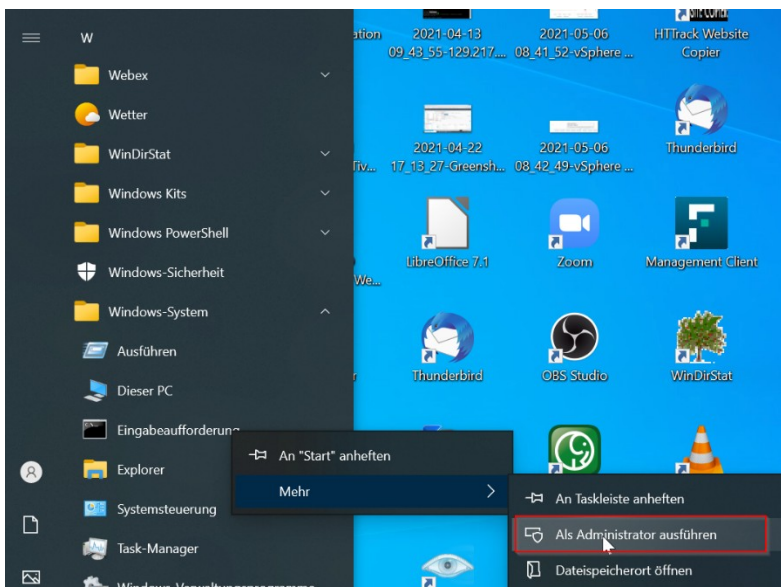
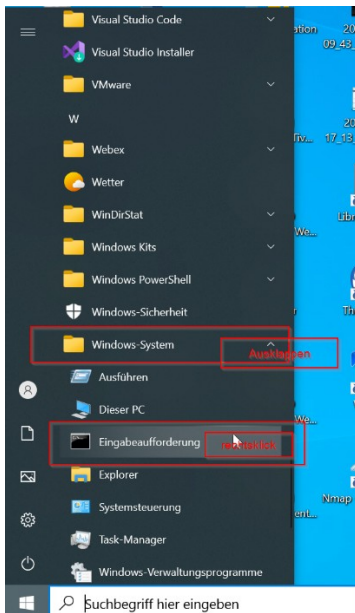


## Manuelle Sicherheitseinstellung für die Sicherheitslücke vom 1.6.2022 (Follina) in Windows und Office

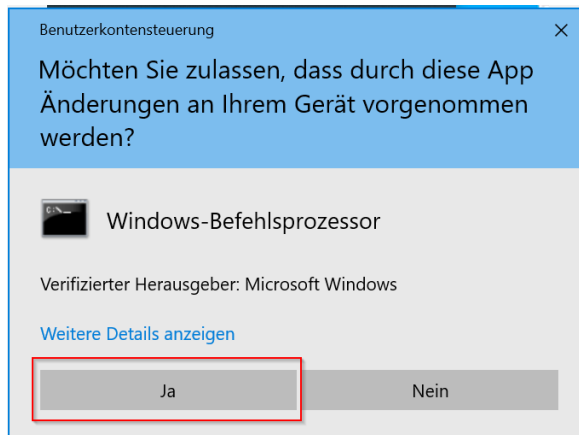
**Diese manuelle Einstellung ist nur erforderlich, wenn Ihr PC nicht in der TU-Domäne oder nicht von Ihrer Fakultät verwaltet wird.**

Stand der Info: 2.6.2022

- Öffnen Sie die Startleiste mit dem Windowssymbol links unten mit einem Klick
- Scrollen Sie bis zum Eintrag „Windows System“
- Klappen Sie den Ordner auf und klicken mit der **rechten Maustaste** auf „Eingabeaufforderung“ und schieben Sie die Maus auf „mehr“, dann klappt die Option „als Administrator ausführen“ aus, klicken Sie hier mit der linken Maustaste:

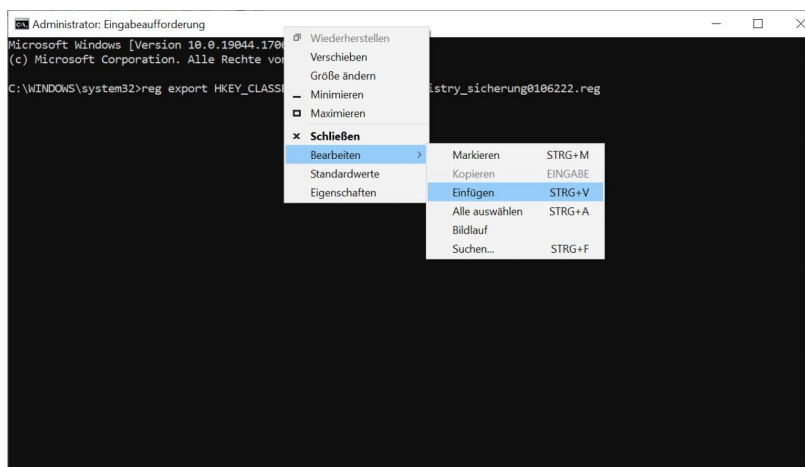


- d) Wenn Sie die Option „Als Administrator ausführen“ nicht finden oder diese bei Ihnen ausgegraut ist, wenden Sie sich bitten an Ihren lokalen IT-Betreuer oder an das ITMC.
- e) Bestätigen sie den folgenden Dialog:



- f) Geben Sie auf der Kommandozeile folgenden Befehl gefolgt von der Enter-Taste (Eingabetaste) ein. Sie sollten die Befehle per Cut&Paste (Strg-C kopieren) in die Kommandozeile einfügen, indem Sie dort mit der rechten Maustaste auf die Titelleiste klicken und „Bearbeiten“ „Einfügen“ auswählen, um Fehler zu vermeiden:

```
reg export HKEY_CLASSES_ROOT\ms-msdt c:\registry_sicherung0106222.reg
```



- g) Es wird „Dieser Vorgang wurde erfolgreich beendet“ angezeigt. Bei einer anderen Anzeige wenden Sie sich an Ihren PC-Betreuer. Die Unterstriche in der Zeile sind keine Leerzeichen. Geben Sie nun auch noch diesen Befehl ein
- ```
reg delete HKEY_CLASSES_ROOT\ms-msdt /f
```

Auch hier wird „Dieser Vorgang wurde erfolgreich beendet“ angezeigt. Bei einer anderen Anzeige wenden Sie sich an Ihren PC-Betreuer oder das ITMC.

- h) Geben Sie nun auch noch diesen Befehl (ohne Zeilenumbrüche) ein:

```
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\ScriptedDiagnostics" /v EnableDiagnostics /t REG_DWORD /d 0 /f
```

Auch hier wird „Dieser Vorgang wurde erfolgreich beendet“ angezeigt. Bei einer anderen Anzeige wenden Sie sich an Ihren PC-Betreuer oder das ITMC.

- i) Geben Sie nun auch noch diesen Befehl ein:

```
reg export HKEY_CLASSES_ROOT\search-ms C:/registry_sicherung0206222.reg
```

Auch hier wird „Dieser Vorgang wurde erfolgreich beendet“ angezeigt. Bei einer anderen Anzeige wenden Sie sich an Ihren PC-Betreuer oder das ITMC.

- j) Geben Sie nun auch noch diesen Befehl ein:

```
reg delete HKEY_CLASSES_ROOT\search-ms /f
```

**Ihr Rechner ist nun geschützt!** Sie können das schwarze Fenster der Eingabeaufforderung nun schließen.

## Rückgängig machen der Änderungen

Erst wenn Sie **später aufgefordert werden** die Änderung rückgängig zu machen, gehen Sie folgendermaßen vor: Öffnen Sie wie oben beschrieben die Eingabeaufforderung und geben Sie die folgenden Kommandos ein:

```
reg import c:\registry_sicherung0106222.reg
```

Es wird „Dieser Vorgang wurde erfolgreich beendet“ angezeigt. Bei einer anderen Anzeige wenden Sie sich an Ihren PC-Betreuer. Und das Kommando:

```
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\ScriptedDiagnostics" /v EnableDiagnostics /t REG_DWORD /d 1 /f
```

Es wird „Dieser Vorgang wurde erfolgreich beendet“ angezeigt. Bei einer anderen Anzeige wenden Sie sich an Ihren PC-Betreuer.

```
reg import c:\registry_sicherung0206222.reg
```

Es wird „Dieser Vorgang wurde erfolgreich beendet“ angezeigt. Bei einer anderen Anzeige wenden Sie sich an Ihren PC-Betreuer.

Ihr PC ist nun wieder im Ursprungszustand.

Das Sicherheits-Informationen-Centrum des ITMC

info.sic@tu-dortmund.de