Schutzmaßnahmen vor Ransomware

Das Ziel dieser Anleitung besteht darin, die Makroausführung per Richtlinie zu deaktivieren und Office 2016 auf den neuesten Stand zu bringen um sich somit etwas gegen Ransomware (z.B. Locky, Cryptolocker, Petya) zu schützen.

Des Weiteren sollte die UAC eingeschaltet sein und zur täglichen Arbeit empfehle ich die Benutzung eines Benutzers ohne administrativen Rechte. Ein geeigneter Virenschutz mit integrierter Firewall wäre vorteilhaft. Weiter unten mehr zu diesen Themen.

Voraussetzung: Windows Versionen ab der Prof. Edition. Erst diese besitzen den Gruppenrichtlinieneditor.

Download-Quelle:

Office 365/2016:

https://www.microsoft.com/en-us/download/details.aspx?id=49030

Für weitere Office-Versionen:

Office 2010:

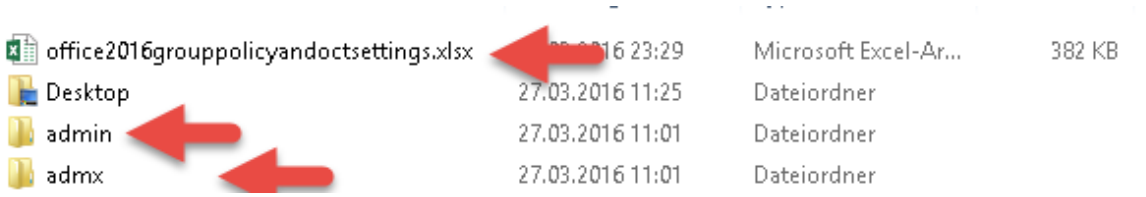
https://www.microsoft.com/en-us/download/details.aspx?id=18968

Office 2013.

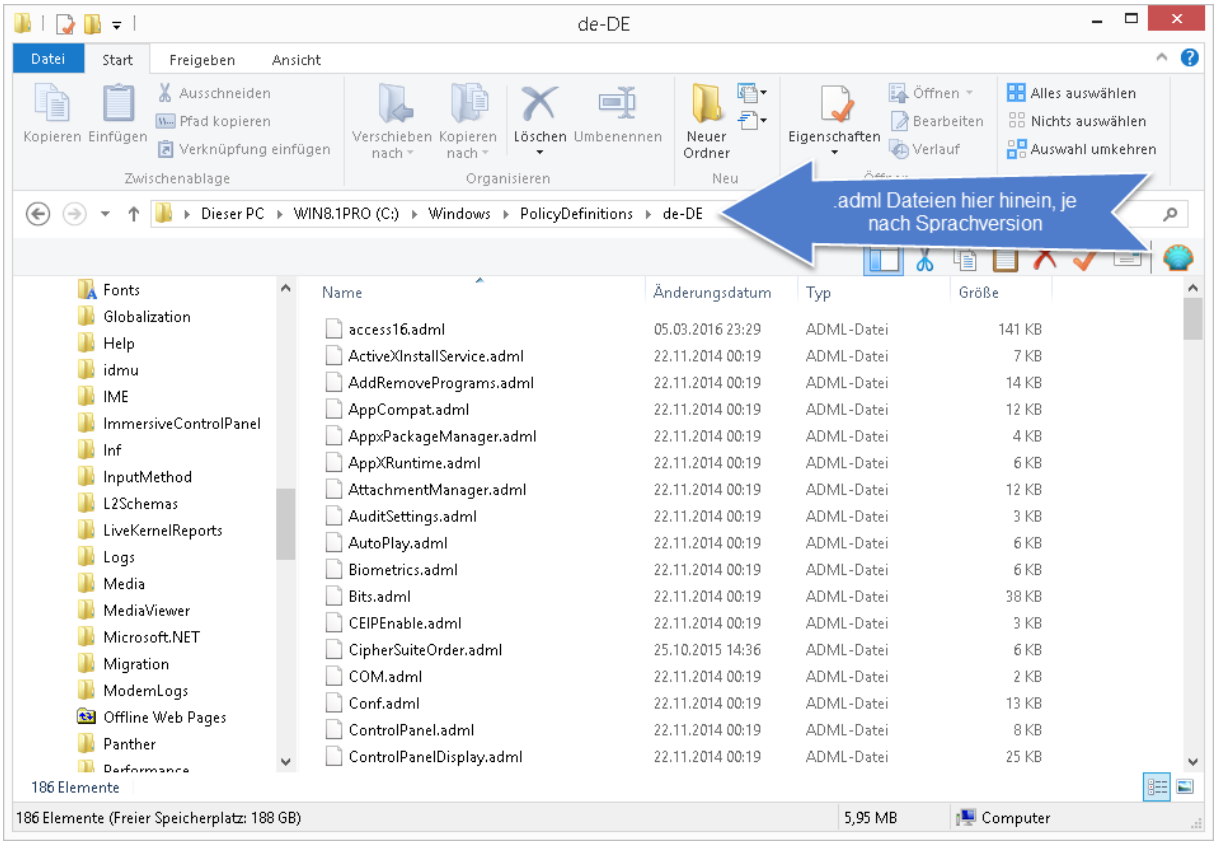
https://www.microsoft.com/en-us/download/details.aspx?id=35554

Nach einem Doppelklick entpackt sich das Archiv „Default" nach C:\Users\%username%

Folgende Datei und Ordner gehören zum Archiv:

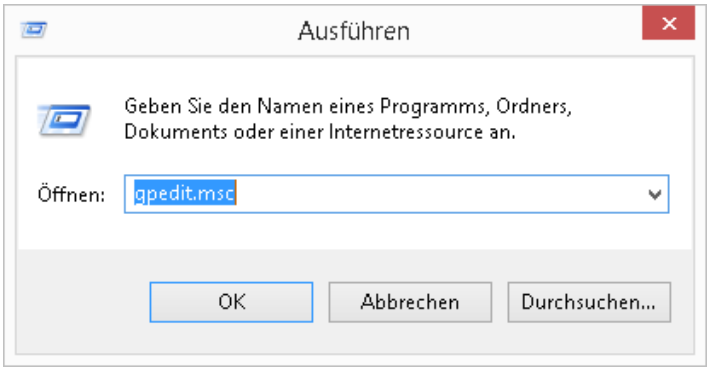


Aus dem Ordner admx unter C:\Users\%username%\admx\de-de kopieren wir die .adml Dateien nach C:\Windows\PolicyDefinitions\de-DE



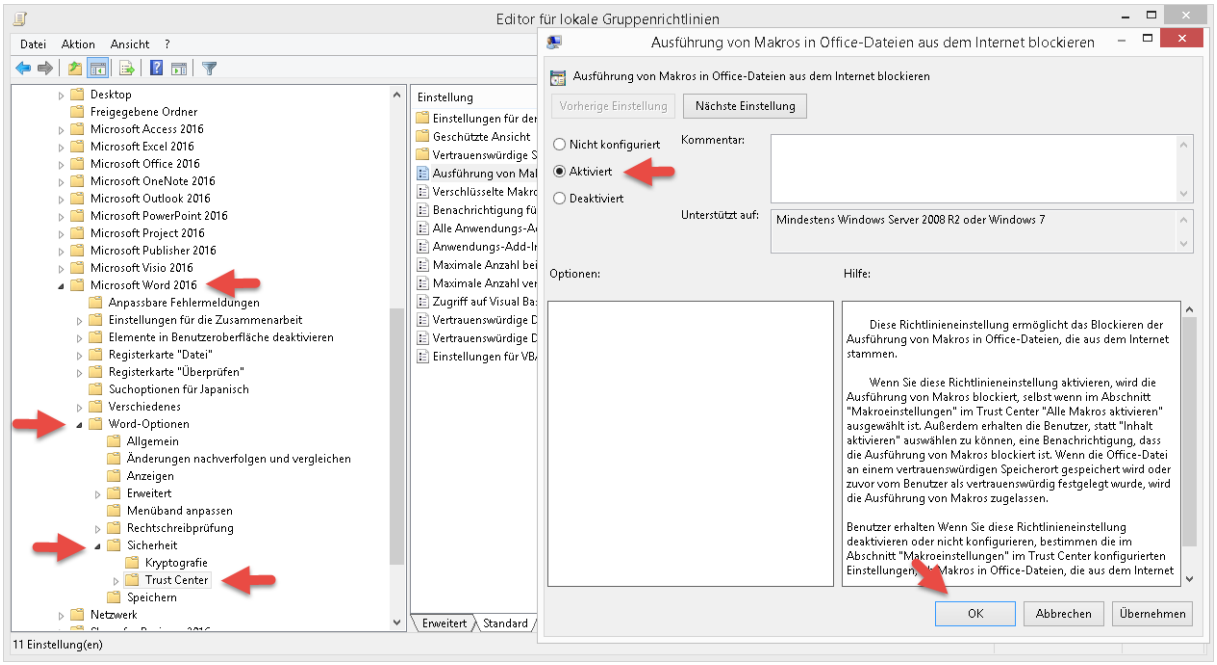
Und aus dem Ordner admx unter C:\Users\%username%\admx kopieren wir alle .admx Dateien nach C:\Windows\PolicyDefinitions.

Jetzt öffnen wir den **Gruppenrichtlinieneditor** in dem wir **Windows + R** oder Ausführen… den Befehl **gpedit.msc** absetzen.

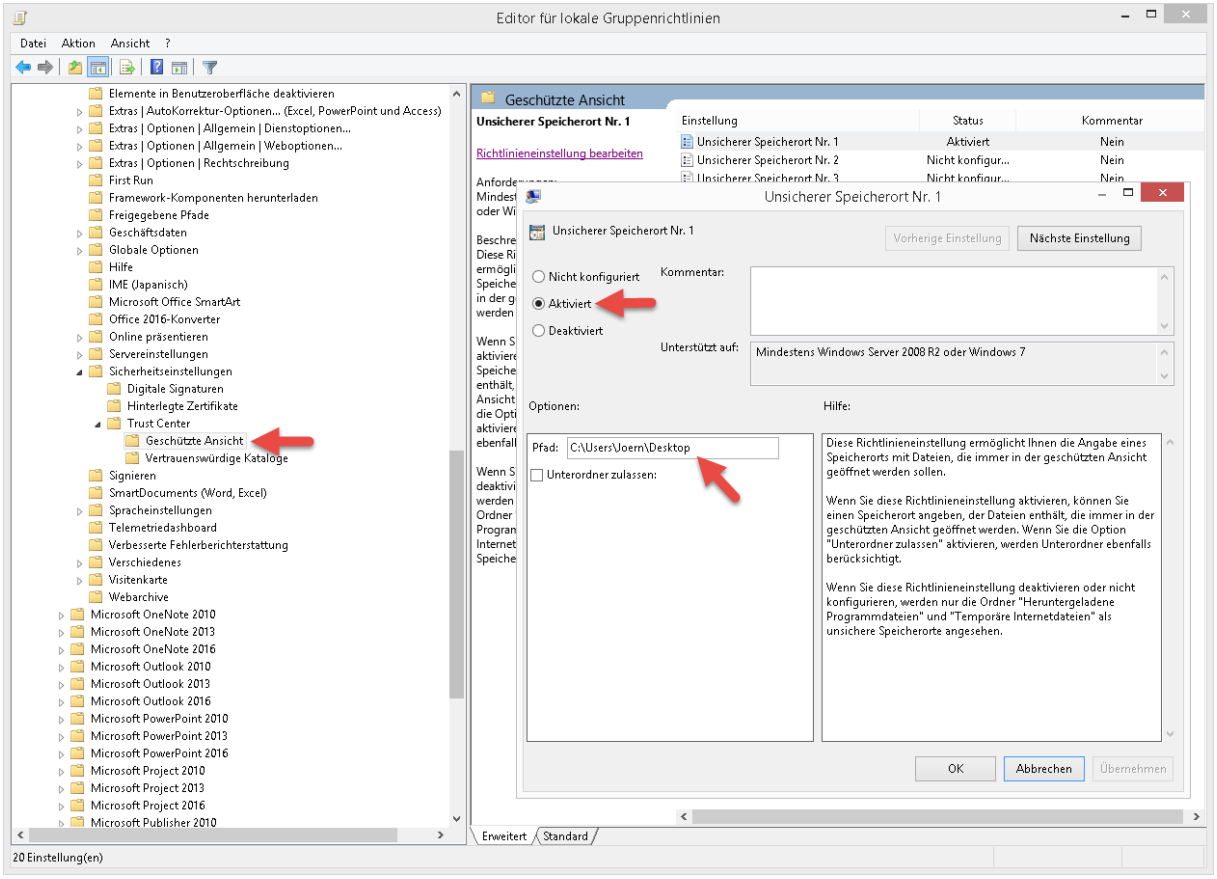


Navigieren über Benutzerkonfiguration > Administrative Vorlagen > Microsoft Word > Word-Optionen > Sicherheit zu Trust Center und aktivieren die Policy „Ausführung von Makros in Office-Dateien aus dem Internet blockieren“ und bestätigen mit einem Klick auf > OK.

Schutzmaßnahmen vor Ransomware



Navigieren über Benutzerkonfiguration > Administrative Vorlagen > Microsoft Office 2016 > Sicherheitseinstellungen > Trust Center zu Geschützte Ansicht und tragen dort die unsicheren Speicherorte ein.

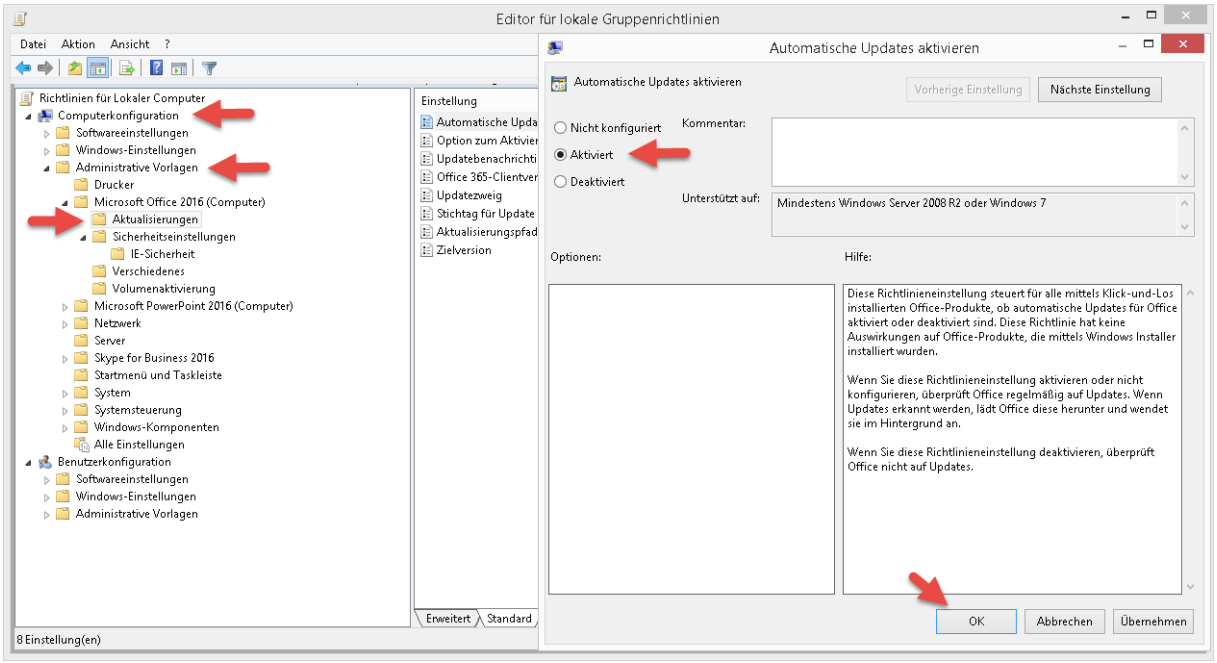


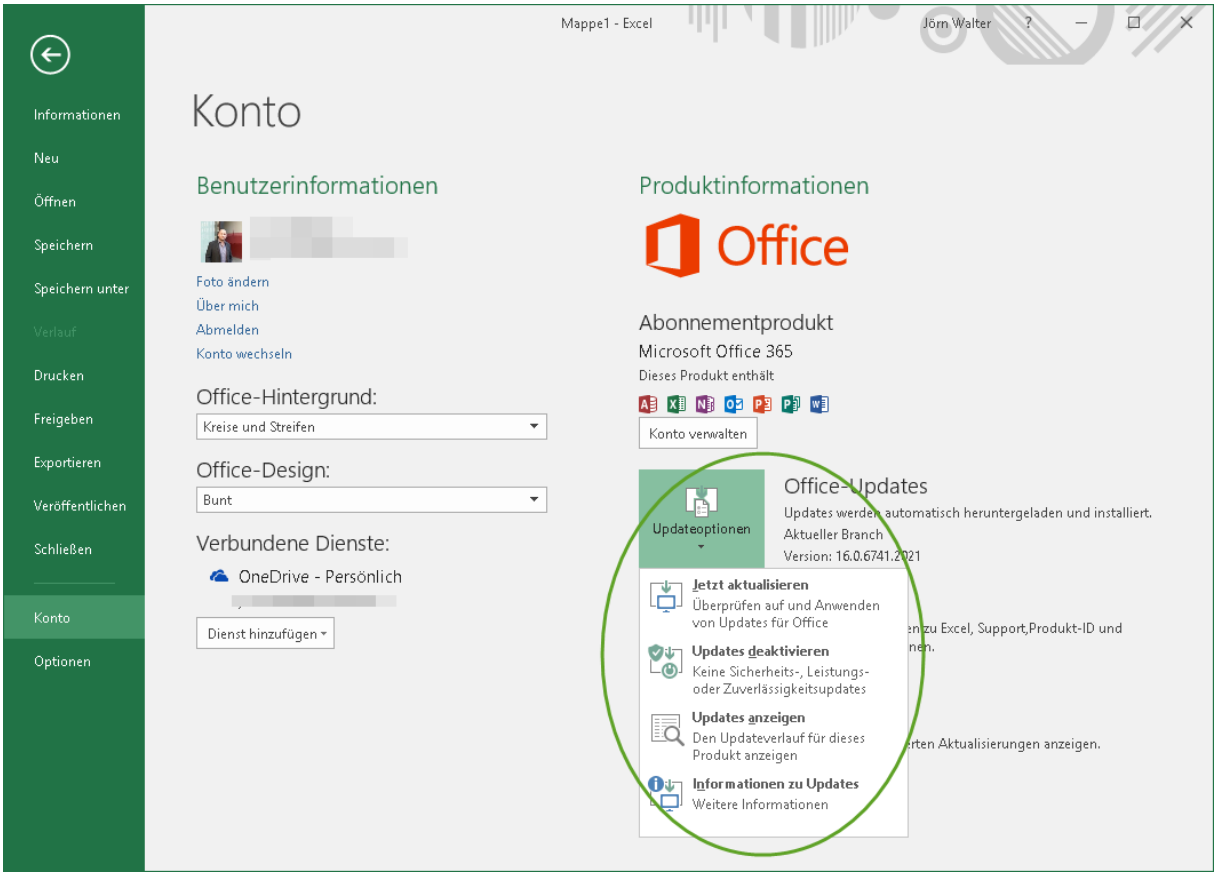
Erstellt von Jörn Walter www.der-windows-papst.de – 23.03.2016

Als nächstes aktivieren wir die automatischen Updates für Office 2016.

Dazu navigieren wir über Computerkonfiguration > Administrative Vorlagen zu Aktualisierungen und aktivieren die Policy „Automatische Updates aktivieren".

Deaktivieren die Policys „Option zum Aktivieren oder Deaktivieren von Updates ausblenden" sowie „Updatebenachrichtigung ausblenden".



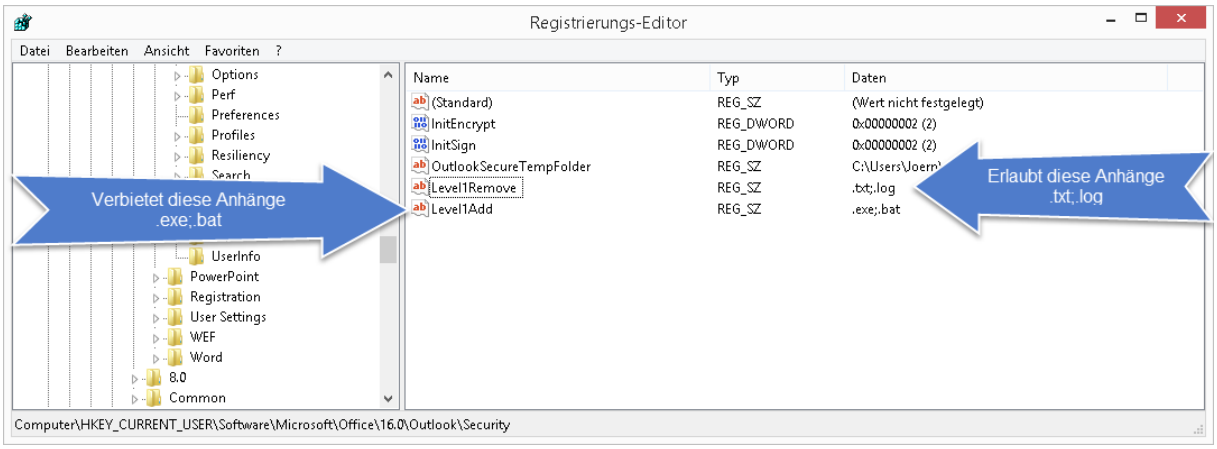


In **Office 2010/2013** gibt es diese Policys noch nicht.

Trotzdem empfehle ich für ALLE Office-Versionen/Systeme noch folgende Einstellungen:

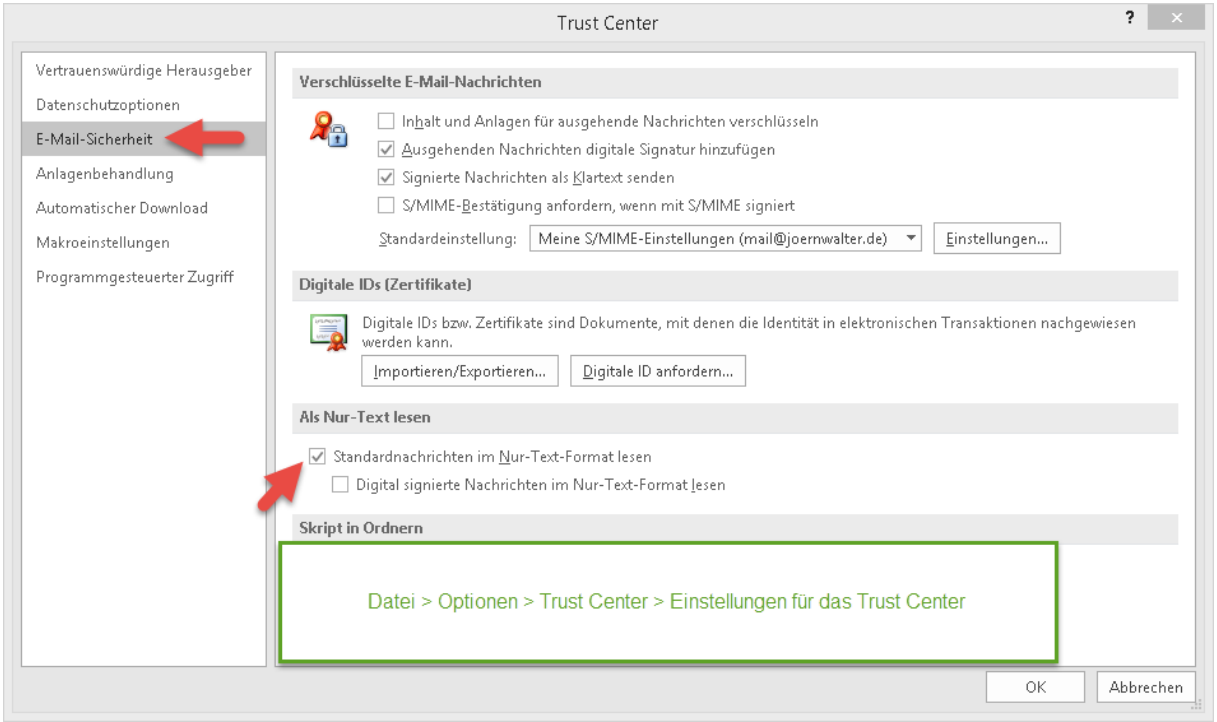
Outlook: Schutz vor nicht gewollten Anhängen

Über die Registry können wir einstellen, welche Anhänge gesehen oder nicht angezeigt werden können/sollen.



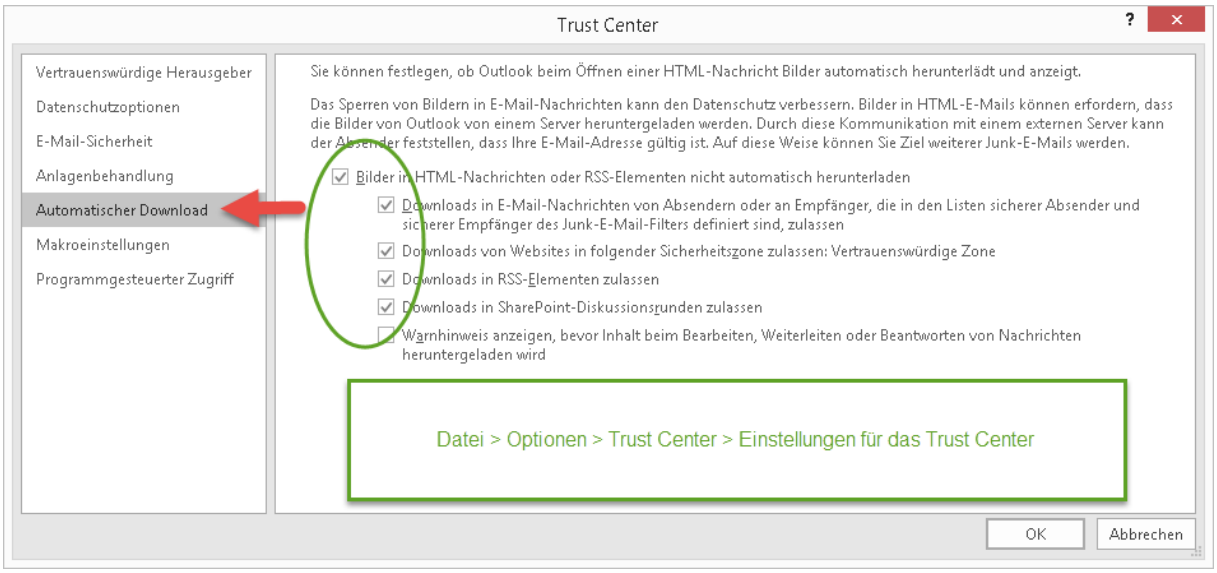

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Security]
"Level1Remove"=".txt;.log"
"Level1Add"=".exe;.bat"
```

Outlook: E-Mail-Sicherheit



Schutzmaßnahmen vor Ransomware

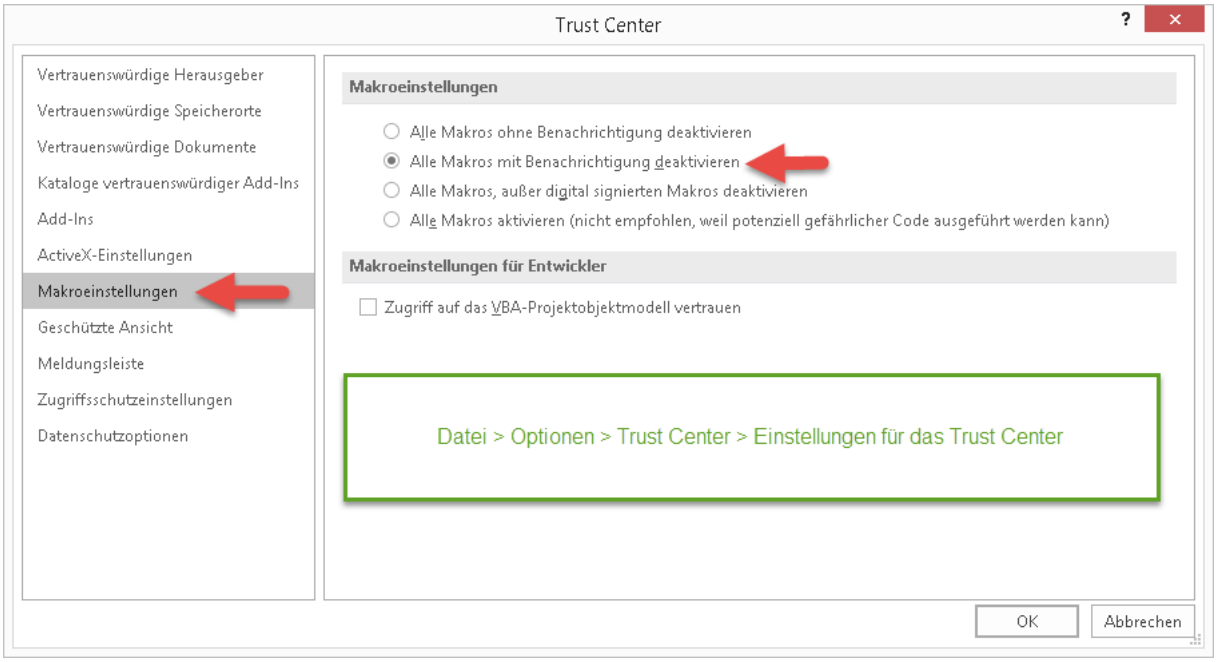
Outlook: Automatischer Download



Weiterführende Informationen zu Anhängen:

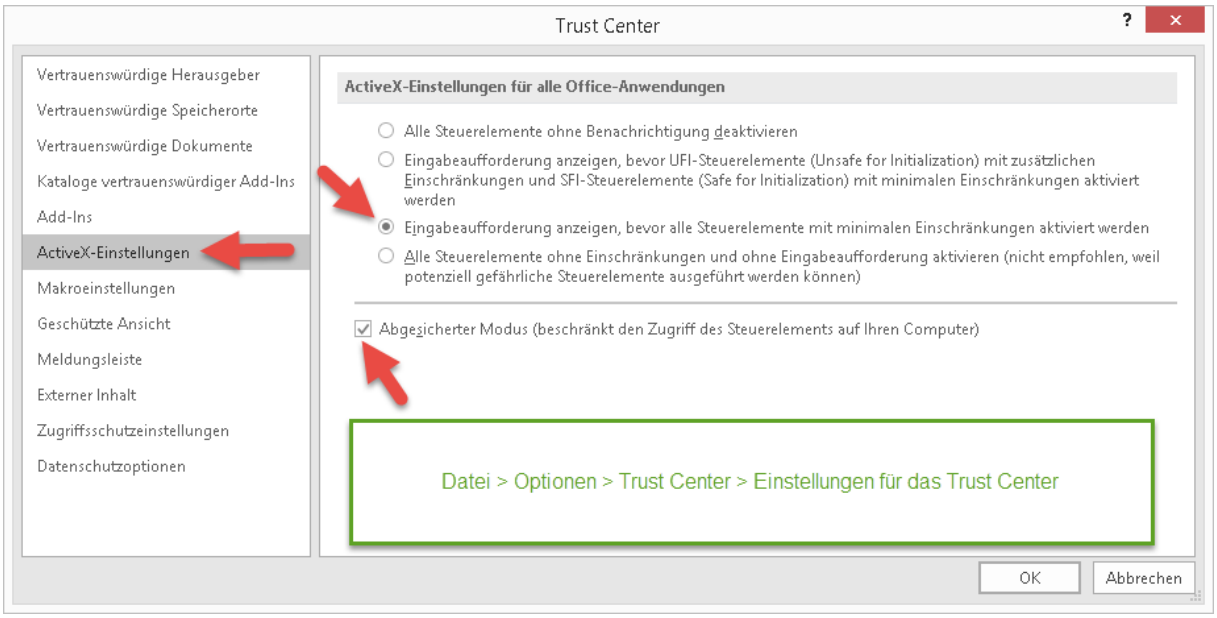
https://support.office.com/en-us/article/Blocked-attachments-in-Outlook-3811cddc-17c3-4279-a30c-060ba0207372?ui=en-US&rs=en-US&ad=US

Word, Excel, Access, Powerpoint: Makros deaktivieren



Schutzmaßnahmen vor Ransomware

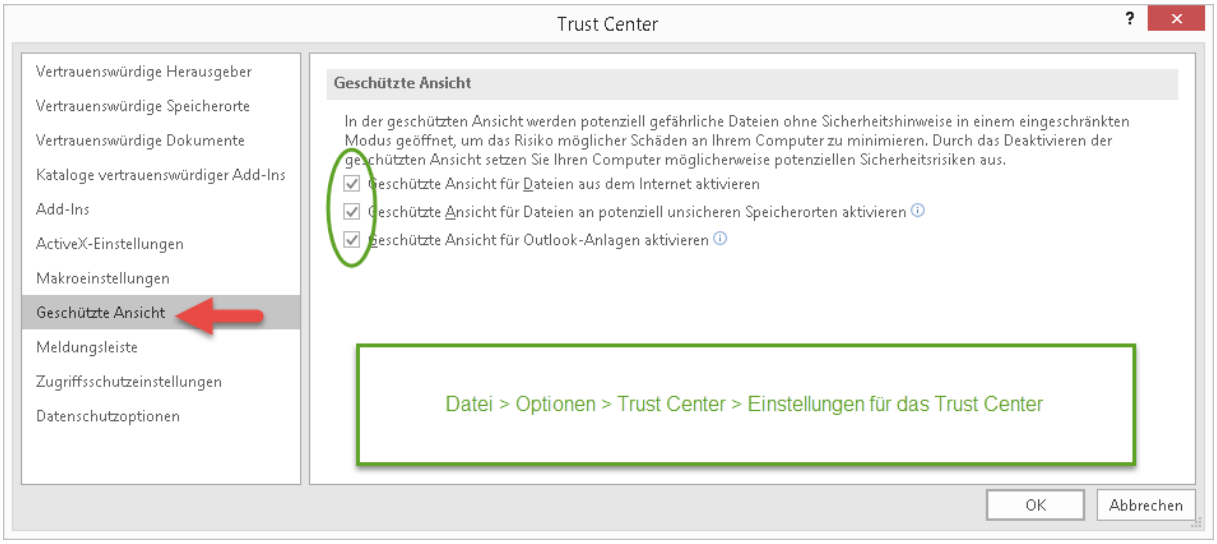
Word, Excel, Access, Powerpoint: ActiveX abgesicherter Modus



Word, Excel, Access, Powerpoint: Geschützte Ansicht

Geschützte Ansicht bedeutet, dass ein Dokument in einer Sandbox geöffnet wird und somit alle Makros ohne Funktion sind. Wird der geschützte Modus über eine Richtlinie verteilt, ist es dem Benutzer nicht möglich diesen Modus zu verlassen. Die Ausführung von Makros wäre dauerhaft untersagt.

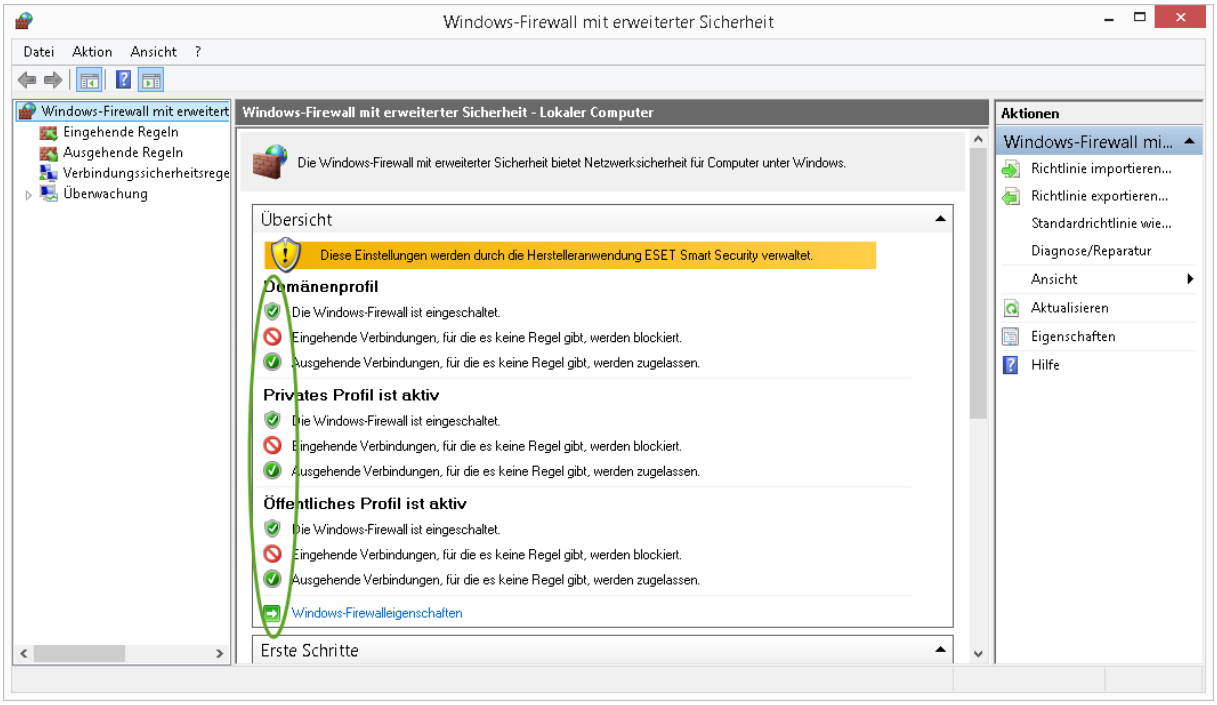
Die Verteilung dieser Einstellung sollte in einem Unternehmen wohl überdacht werden, es gibt Abteilungen wie z.B. Mitarbeiter aus dem Finanz- oder Analytik- Bereich die ohne Makros ihre Arbeit dann nur noch teilweise oder gar nicht erledigen können.



Schutzmaßnahmen vor Ransomware

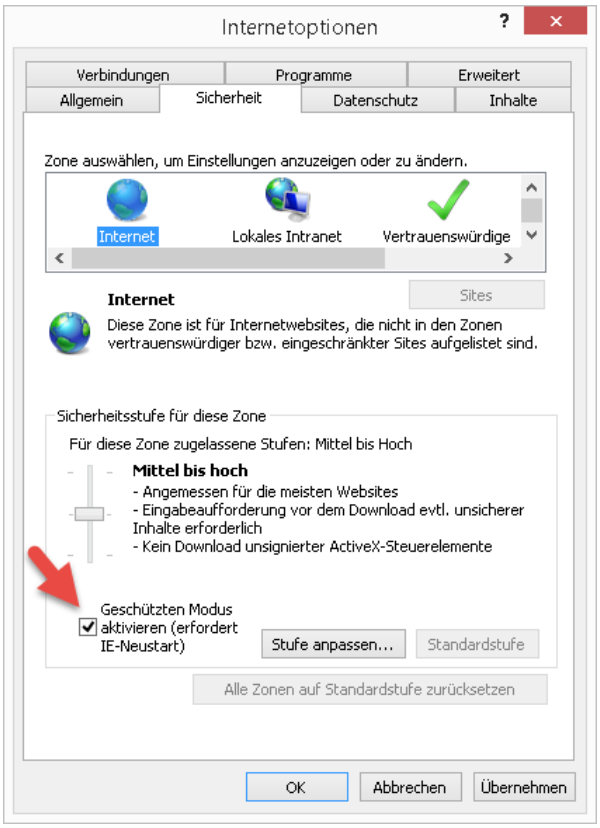
Firewall überprüfen:

Aktiviert jedes Profil; auch wenn ihr in keiner Domäne seit.



Internet Explorer überprüfen:

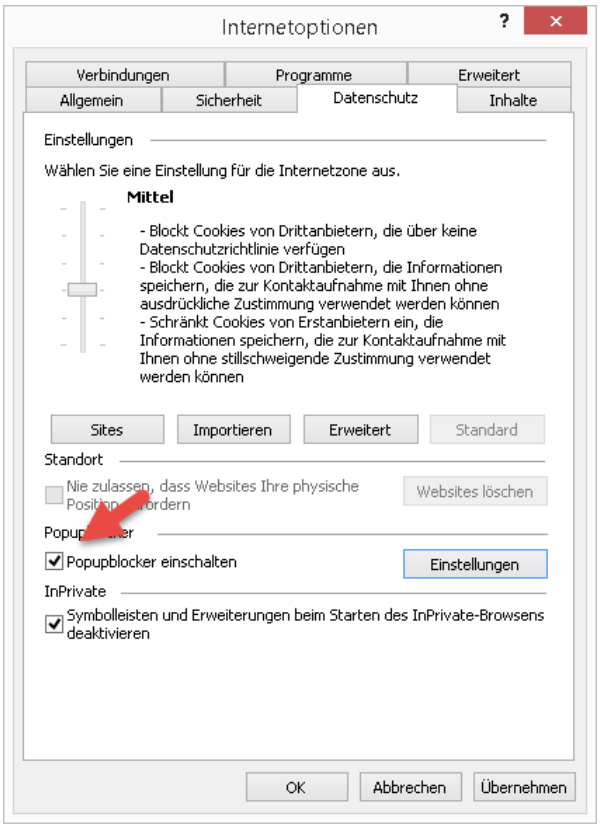
Prüfen ob der “Geschützte Modus” aktiv ist.



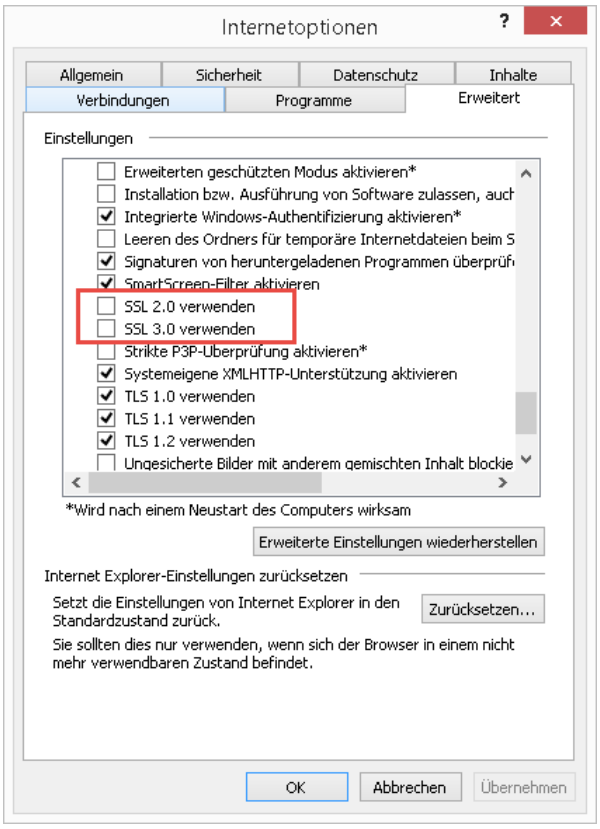
Erstellt von Jörn Walter www.der-windows-papst.de – 23.03.2016

Schutzmaßnahmen vor Ransomware

Popupblocker einschalten:



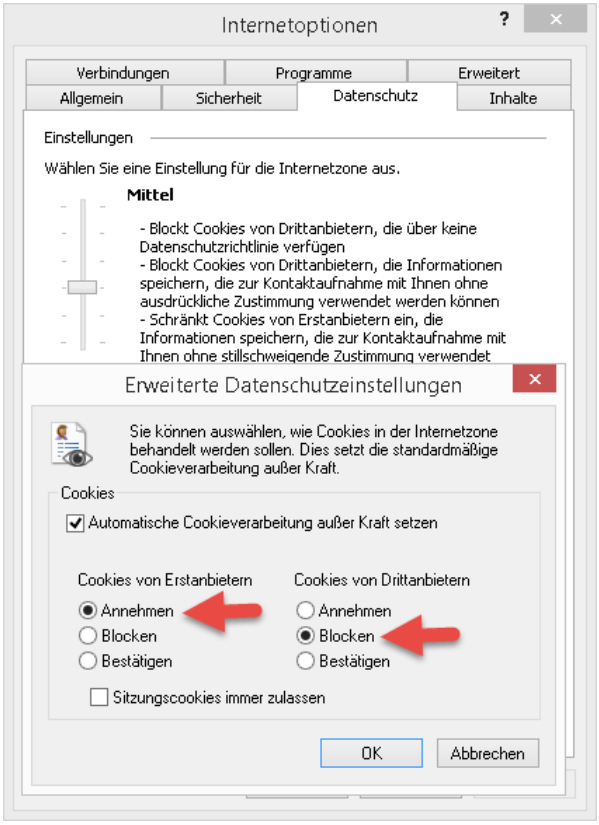
Prüfen ob SSL auch tatsächlich abgeschaltet ist:



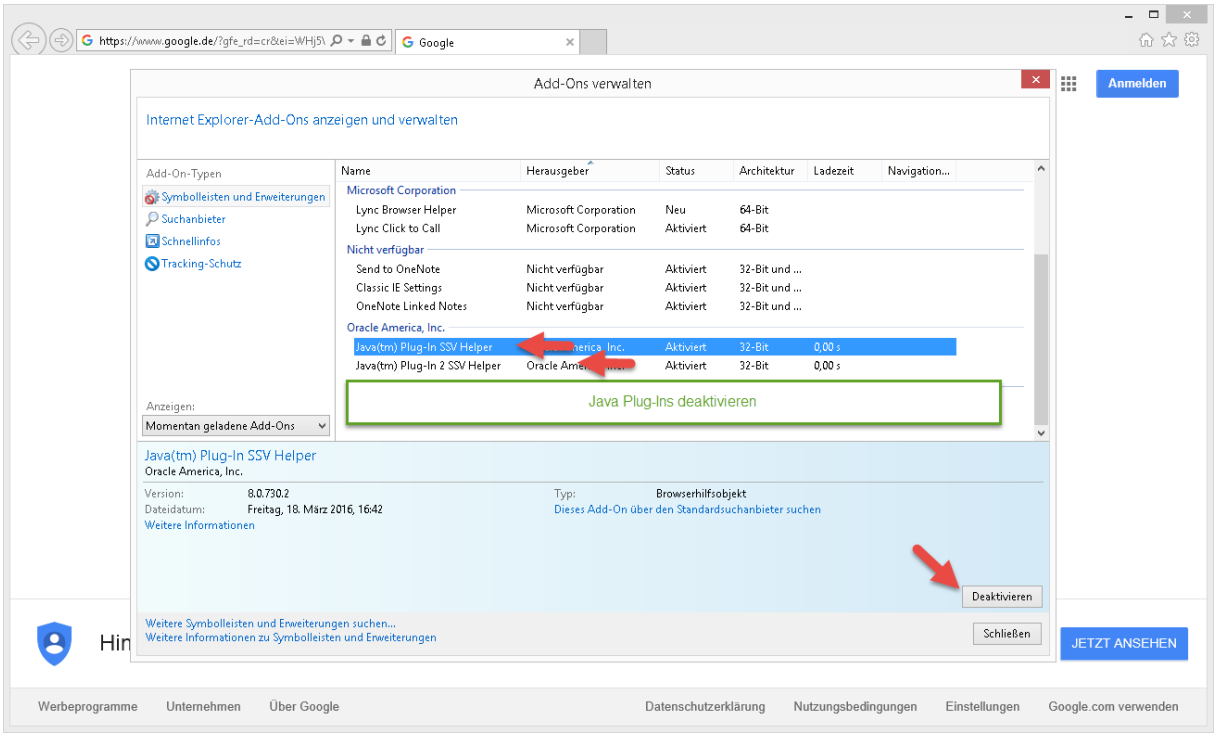
Erstellt von Jörn Walter www.der-windows-papst.de – 23.03.2016

Schutzmaßnahmen vor Ransomware

Drittanbieter Cookies blocken:

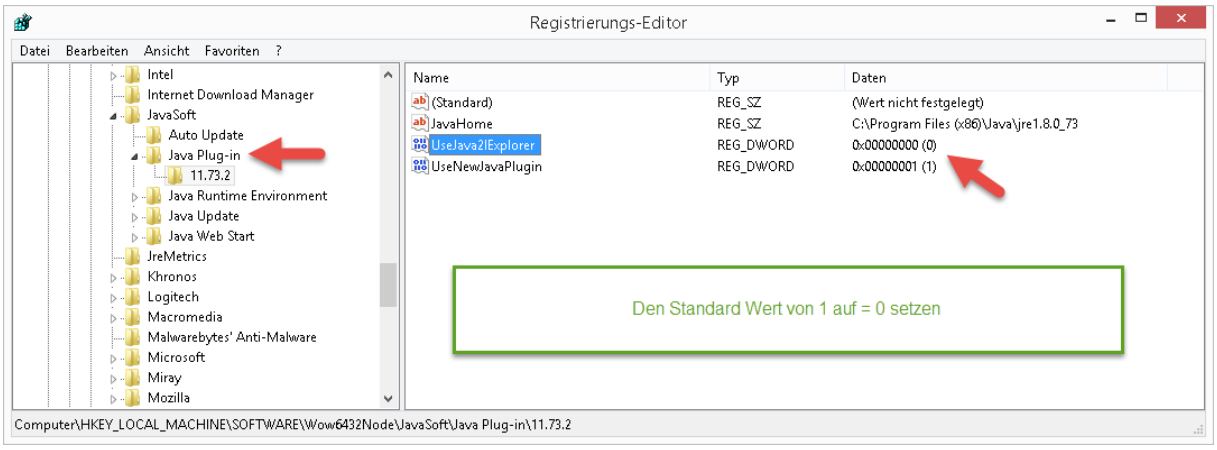


Java Plug-In deaktivieren:



Erstellt von Jörn Walter www.der-windows-papst.de – 23.03.2016

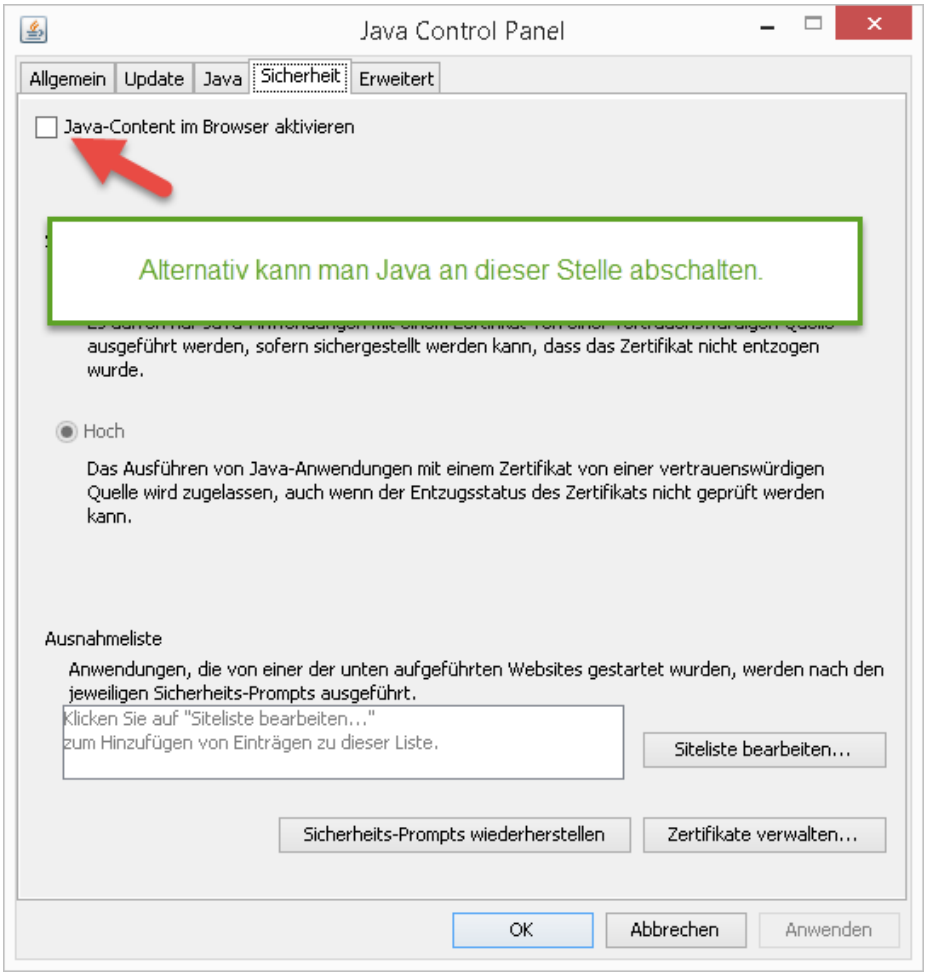
In der Registry noch zusätzlich den Wert 1 auf **0** setzen.



Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\JavaSoft\Java Plug-in\11.73.2]
"UseJava2IExplorer"=dword:0000000**0**

Alternativ kann man Java im Control Panel unter der Systemsteuerung abschalten.

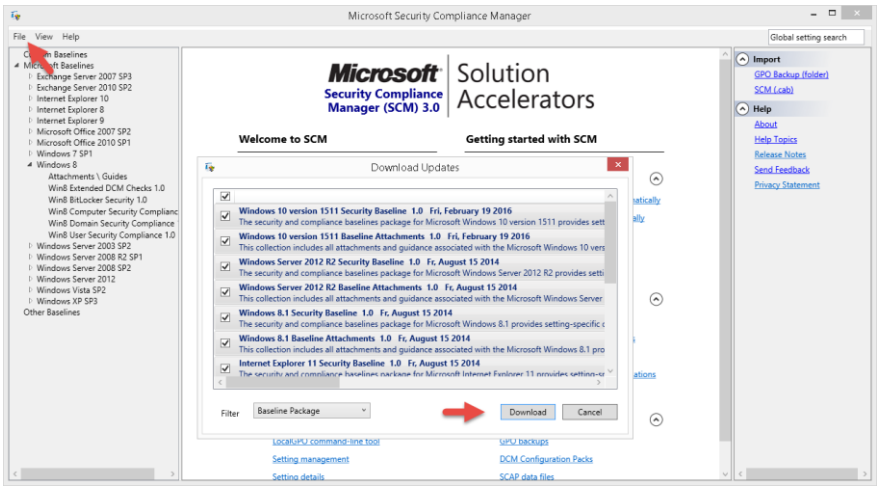


Installiert den Security Compliance Manager SCM 3.0 und überprüft euer System auf Schwachstellen. Nach der Installation bitte erst updaten damit aktuelle Systeme und Konfigurationen unterstützt werden.

Schutzmaßnahmen vor Ransomware

Download:

https://technet.microsoft.com/en-us/solutionaccelerators/cc835245.aspx



Erweitere Maßnahmen - Softwareeinschränkungen:

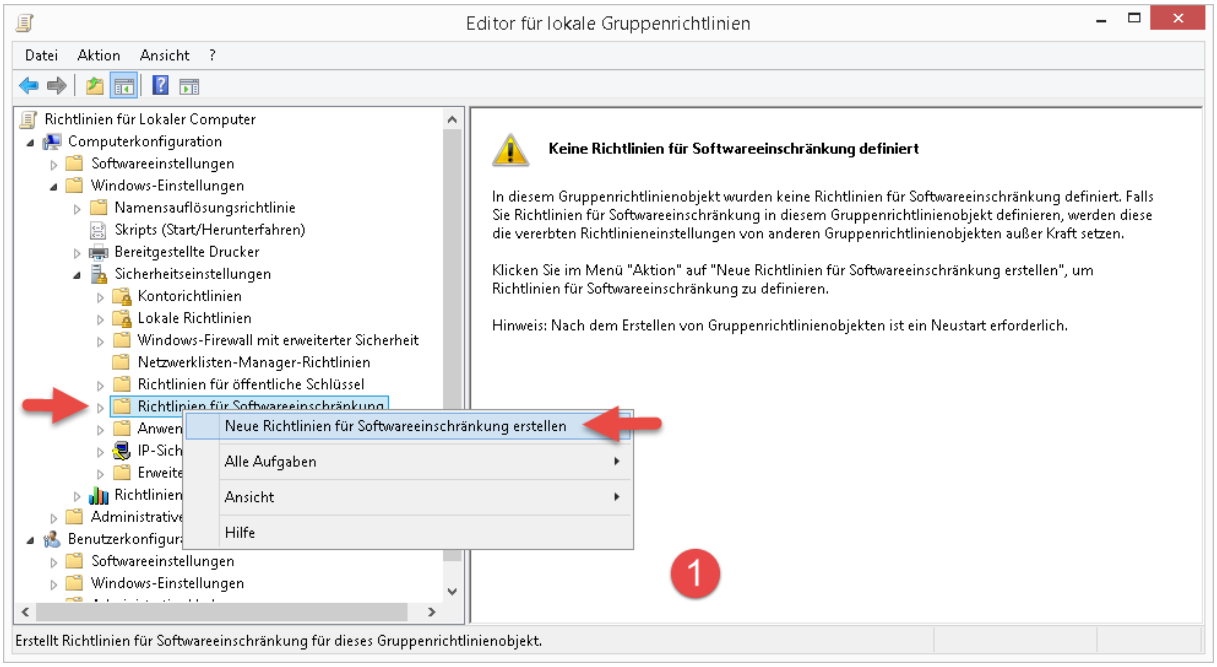
Eine weitere Maßnahme wäre der Schutz lokaler und sensibler Pfade. Dieser Schutz soll verhindern, das Anwendungen die aus dem Internet unbewusst heruntergeladen und extrahiert wurden, gestartet werden können.

Hierzu gehören die Pfade:

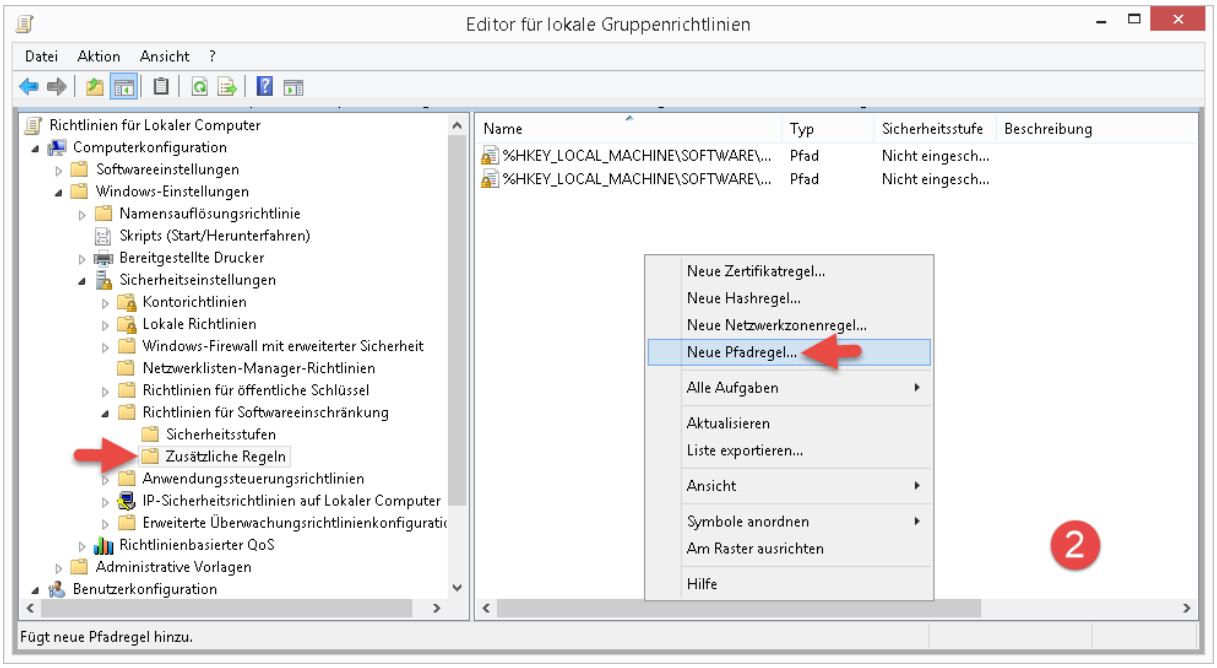
- AppData
- LocalAppData und
- Temp

Wir navigieren im Gruppenrichtlinieneditor zum Pfad: Computerkonfiguration > Windows-Einstellungen > Sicherheitseinstellungen > Richtlinien für Softwareeinschränkungen

Als erstes machen wir einen Rechtsklick Richtlinien für Softwareeinschränkungen um diese erstmalig zu aktivieren. Daraufhin wird die Policy um die Sicherheitsstufen und Zusätzliche Regeln erweitert.

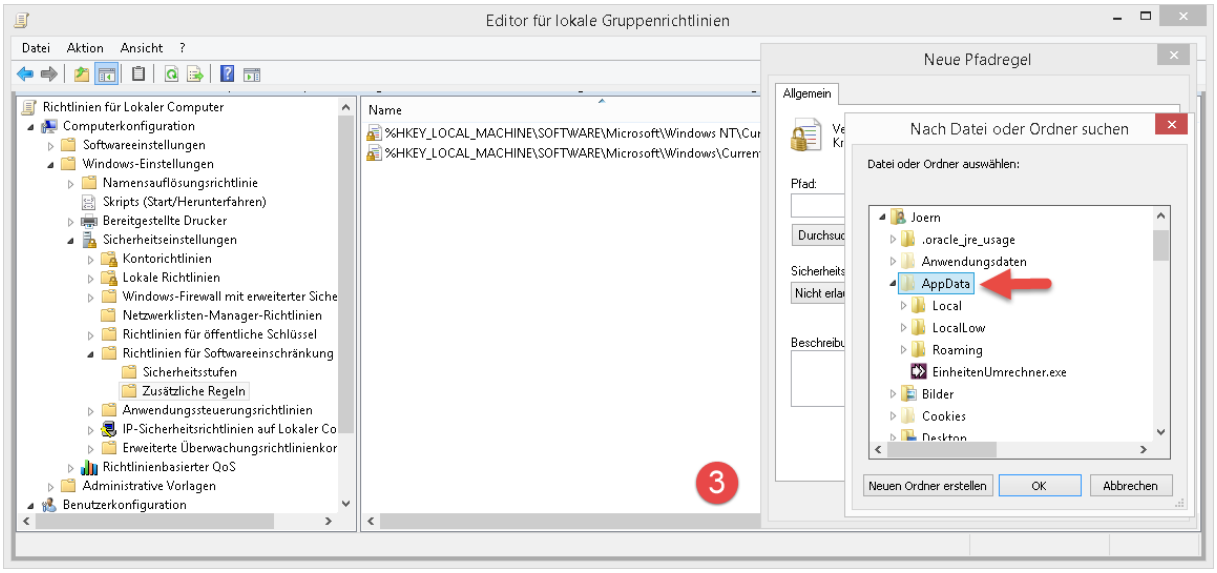


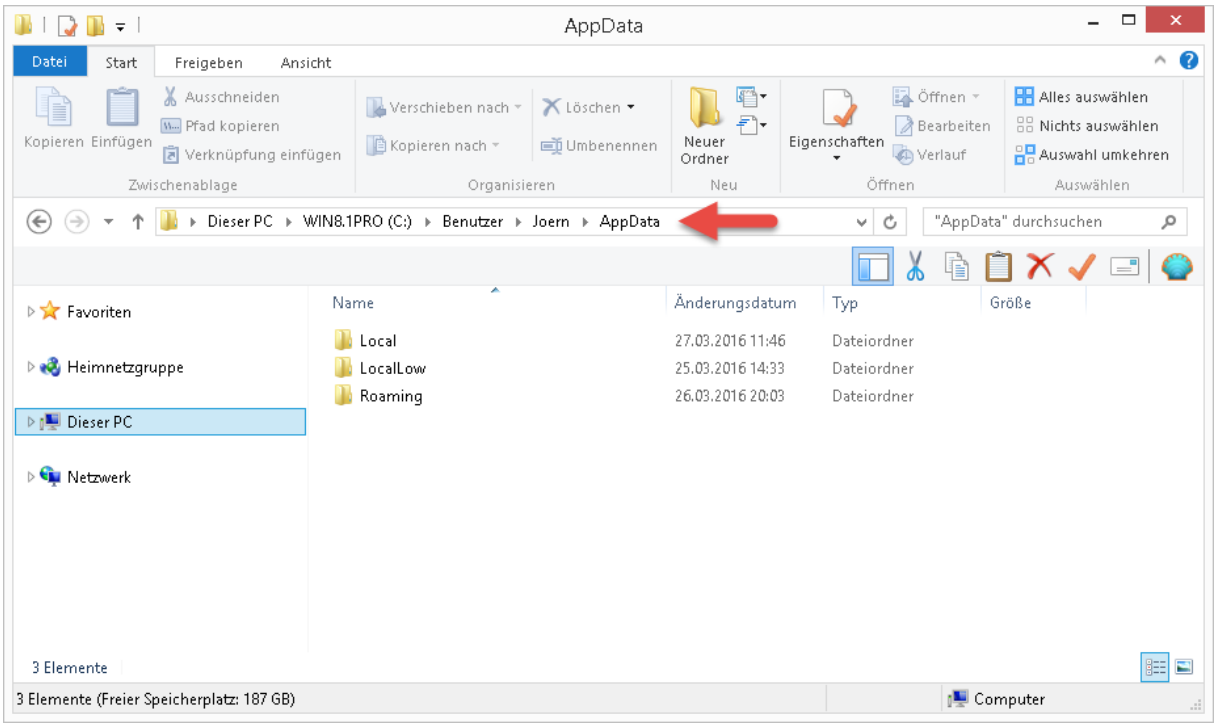
Im nächsten Schritt erstellen wir eine neue Pfadregel und kopieren alle Pfade, aus denen keine Anwendung gestartet werden soll hinein.



Das wäre der Pfad C:\Users\Joern\AppData

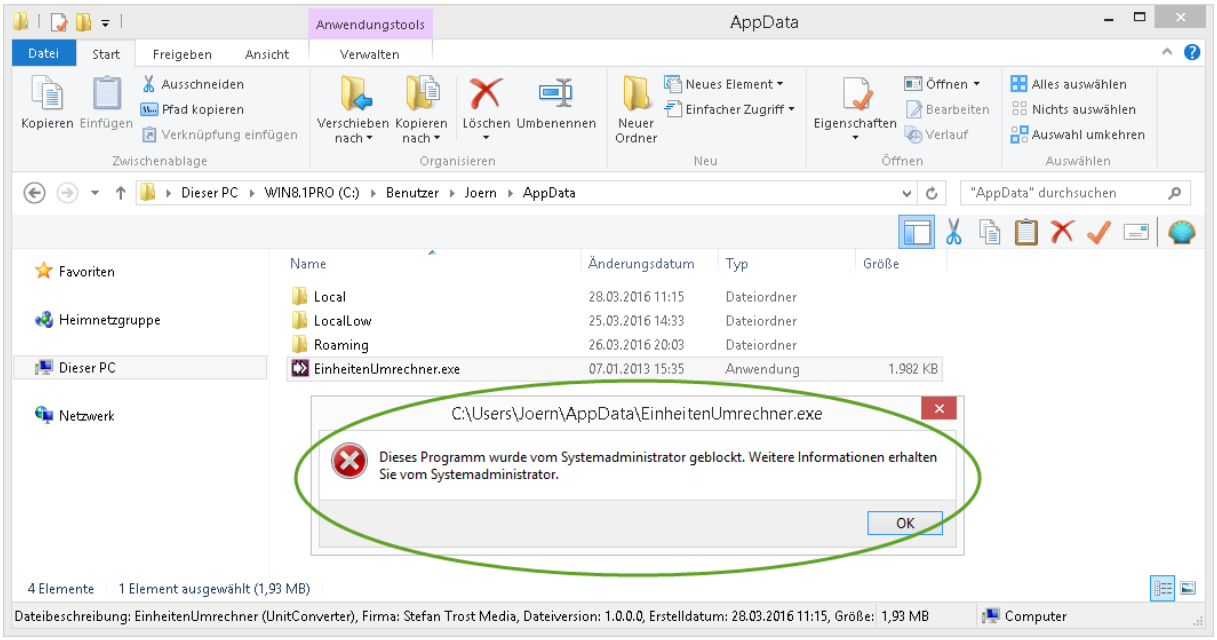
Schutzmaßnahmen vor Ransomware



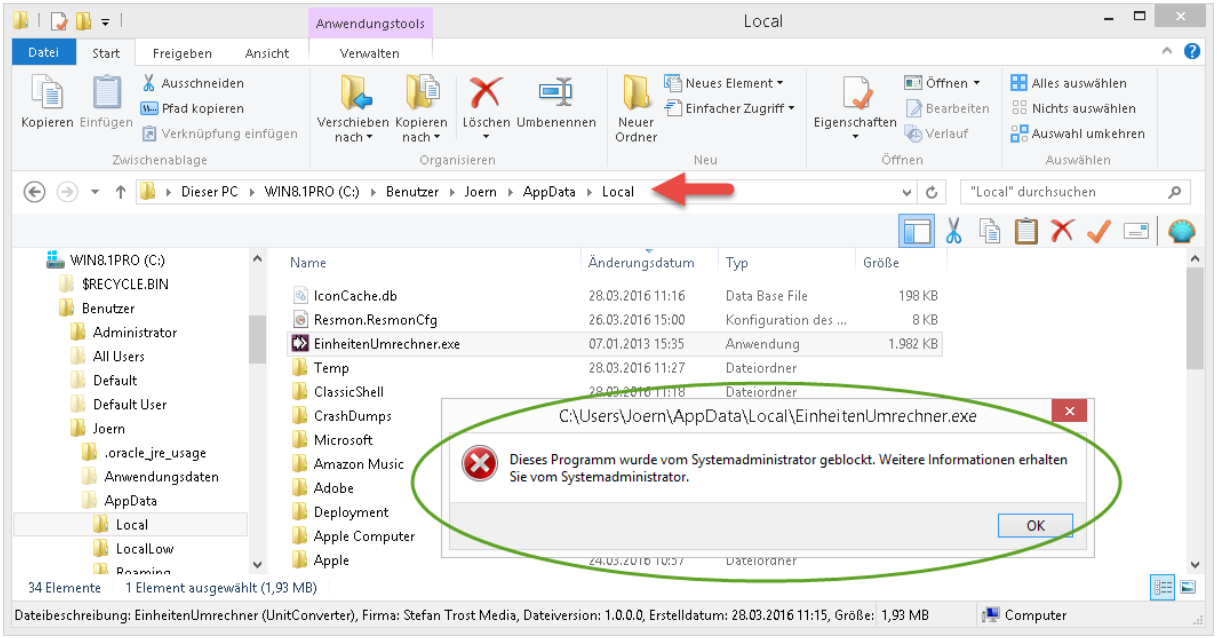


Würde ich jetzt versuchen eine Anwndung auszuführen, die in diesem Pfad abgelegt ist, bekomme ich folgende Warnung angezeigt:

Schutzmaßnahmen vor Ransomware



Auch die Unterordner sind durch diese Policy geschützt.



Hinweis: Wenn ich Anwendungen über die Taskleiste starten möchte, werden auch diese blockiert, teilweise auch Verknüpfungen in Start > Alle Programme!

Wenn ihr euch die Verknüpfungen auf den Desktop legt ist alles gut!

Erstellt von Jörn Walter www.der-windows-papst.de – 23.03.2016

Schutzmaßnahmen vor Ransomware

Ich weiß, Schutzmaßnahmen sind irgendwie immer kontraproduktiv. Die Frage ist nur, was will man letzten Endes erreichen?!

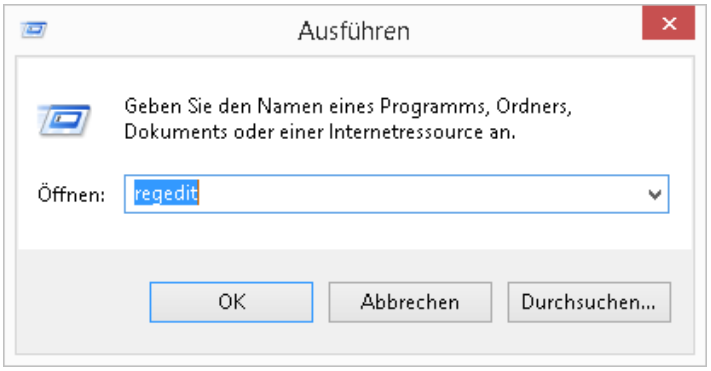
In einer Domäne würde die Richtlinie jetzt auf die Client OU verknüpft werden, wobei der anzuwendenden Pfad dort wie folgt lauten würde:

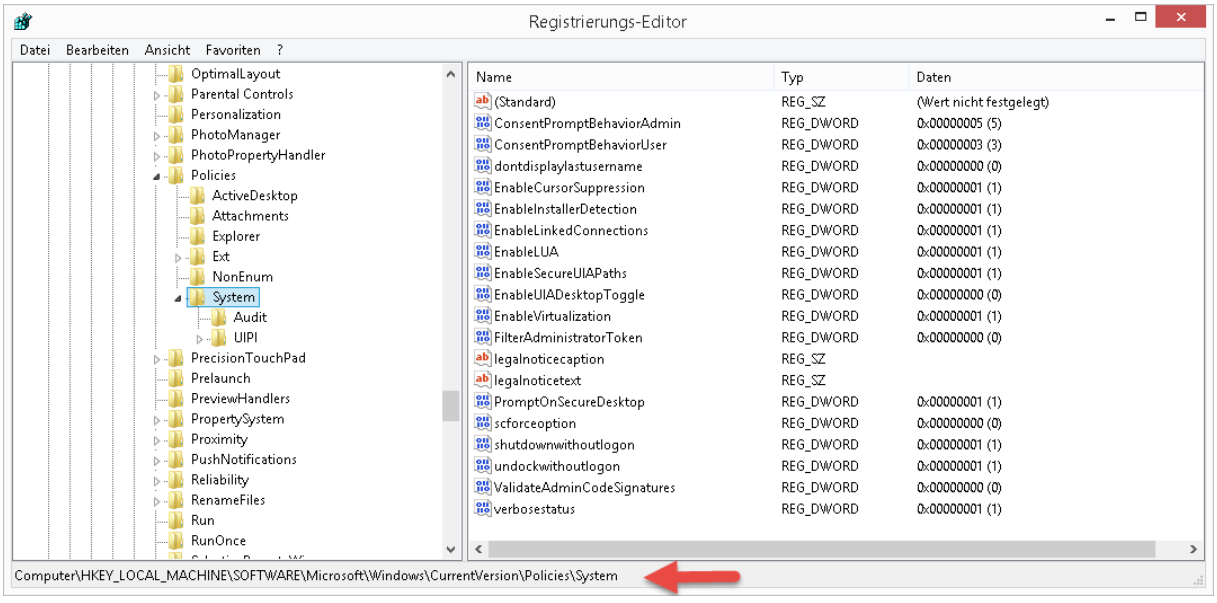
%appdata%*.exe

Die Benutzerkontensteuerung sollte auf diese Werte gestellt werden:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]
"EnableVirtualization"=dword:00000001
"EnableInstallerDetection"=dword:00000001
"PromptOnSecureDesktop"=dword:00000001
"EnableLUA"=dword:00000001
"ConsentPromptBehaviorAdmin"=dword:00000005
"ConsentPromptBehaviorUser"=dword:00000003
"FilterAdministratorToken"=dword:00000001
```

Über **Start > Ausführen** und dem Befehl **regedit** öffnen wir den Registry-Editor.





Optional:

Locky, CRYPTESLA, CRILOCK (Crypto Ransomware) baut auf Word Makros auf und wird häufig per E-Mail an die Opfer verteilt. Pro Stunde verursacht Locky tausende von Infektionen.

Dridex ein Online Banking Schädling wird auf dieselbeweise wie Locky verteilt. Die E-Mail tarnt sich als Rechnung oder als harmlose Nachricht. Beide Schädlinge verweisen auf den Anhang mit der Bitte diesen zu öffnen.

Wird der Anhang geöffnet, startet das enthaltene Makro einen Downloader namens ladybi.exe. Dieser Downloader lädt den Cryptolocker herunter und verschlüsselt vorhandene Daten, vorzugsweise Office Dokumente.

Was macht die Ransomware noch gefährlicher als die Tatsache, dass unsere Daten verschlüsselt werden? Richtig! Sie verändern sich und werden durch unsere Anti-Viren Lösung nicht erkannt oder zu spät erkannt.