SSL 3.0 deaktivieren – Sicherheitslücke „Poodle"

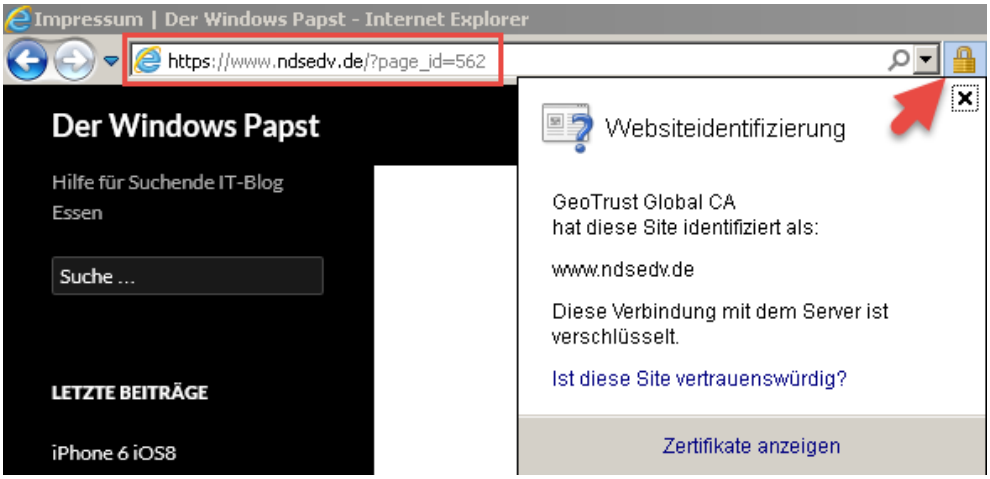
Wie bereits aus den Medien zu entnehmen war, wurde neben den bereits bekannten Lücken Heartblead und Shellschock eine Schwachstelle in SSLv3 gefunden.

Die entdeckte **Lücke** wurde auf den Namen „**Poodle**" getauft.

Das Resultat dieser Lücke ist, das sich der Angreifer über „Poodle" in sichere Verbindungen zwischen der Internetseite und den Besuchern einschleichen Daten abfangen und auslesen kann.

Bei den Daten handelt es sich um gespeicherte Cookies, mit Nutzerinformationen über z.B. soziale Netzwerke, Shopping- und Bankseiten und E-Mail Diensten. Durch diese Attacke verspricht sich der **Hacker** eine Ausbeute an Passwörtern Kredit- oder Kontodaten. -

18 Jahre ist das damals von Netscape entwickelte HTTPS–Protokoll SSL nun alt. Dieses Protokoll dient zur sicheren Übertragung von vertraulichen Informationen.



Aus kompatibilitätsgründen wurde dieses Protokoll bis heute weitergenutzt, obwohl es bereits durch das sichere Protokoll TLS abgelöst wurde.

Wie gehen wir als Nutzer von diversen Browsern mit dieser neuen Sicherheitslücke um und wie können wir uns davor schützen?

Als erstes sind öffentliche W-LAN Hotspots zu vermeiden und vertrauen Sie keinem unbekannten W-LAN welches Sie selbst nicht kontrollieren können.

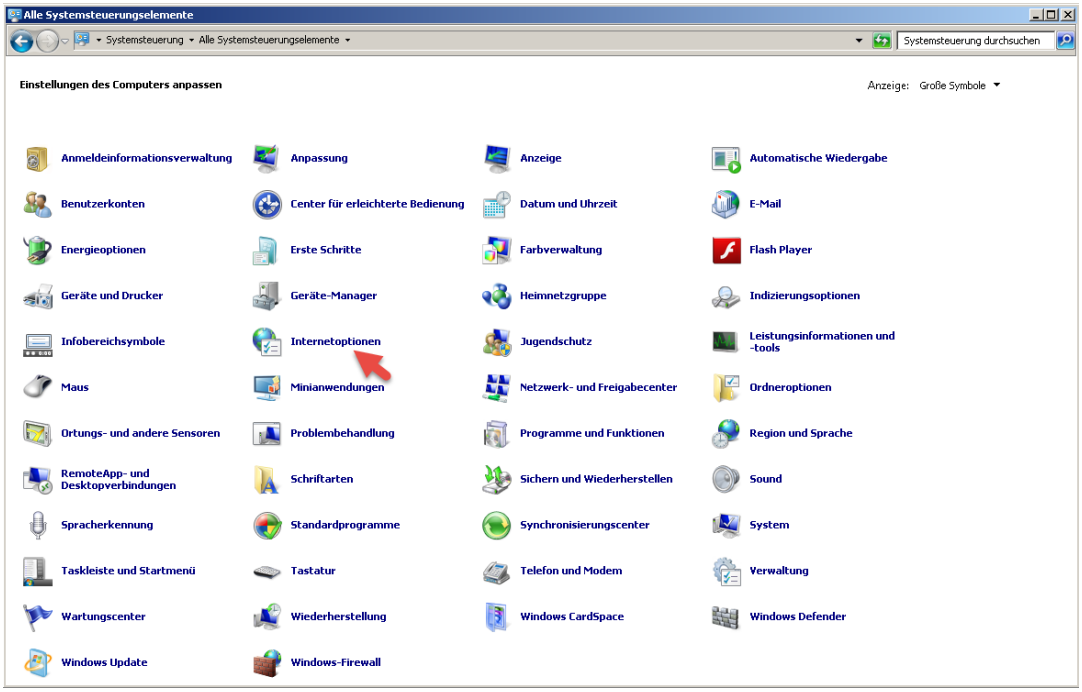
Microsoft empfiehlt die **Abschaltung** des HTTPS-Protokolls **SSLv3** und SSLv2 (Secure Socket Layer).

Deaktivierung von SSL 3.0 im Internet Explorer, Firefox und Chrome.

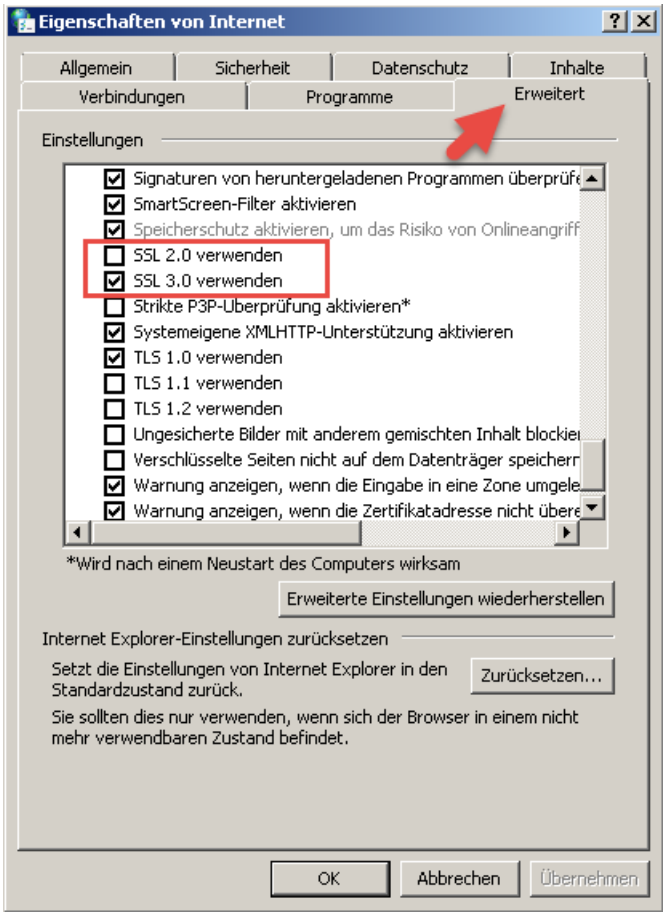
- **Internet Explorer**

Wir öffnen in der Systemsteuerung die Internetoptionen

SSL 3.0 deaktivieren – Sicherheitslücke „Poodle“



Es öffnet sich das **Eigenschaftenfenster**. Unter dem **Reiter > Erweitert** scrollen wir zu den **Sicherheitseinstellungen** bis zu dem Punkt **SSL.**



Wir **entfernen** wenn gesetzt beiden **Haken** in den Kontrollkästchen neben SSL 2.0 und **SSL 3.0**.

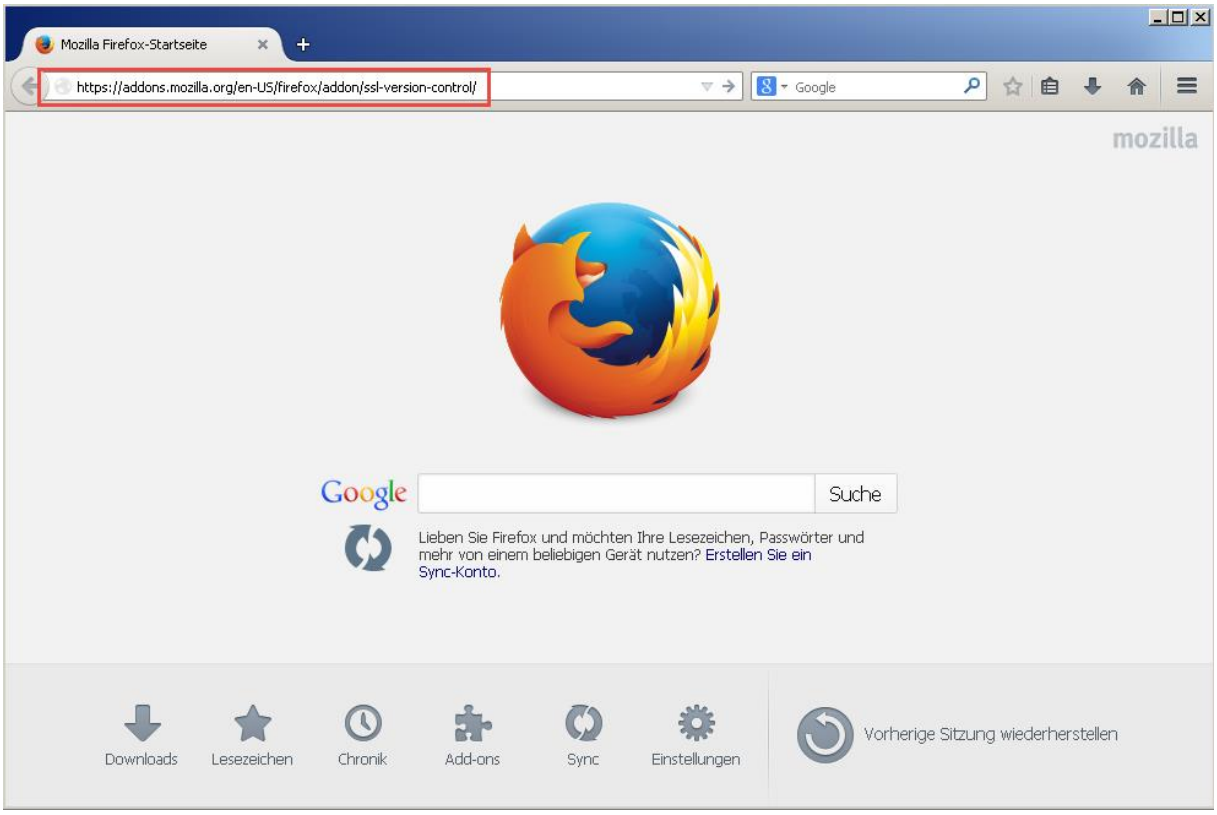
Erstellt von Jörn Walter www.der-windows-papst.de – 17.10.2014

SSL 3.0 deaktivieren – Sicherheitslücke „Poodle"

- **Firefox**

Wir öffnen Firefox und laden uns von folgender Webseite das Add-on **SSL-Version-Control** herunter.

https://addons.mozilla.org/en-US/firefox/addon/ssl-version-control/

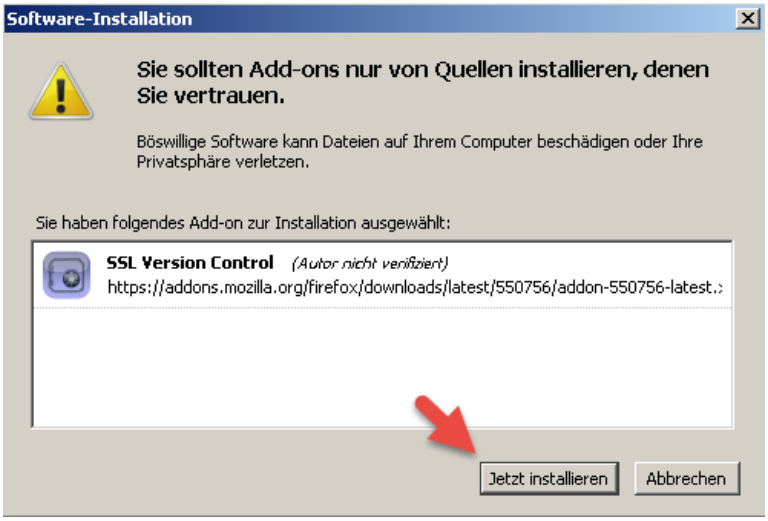


Wir klicken auf **+ Add to Firefox**

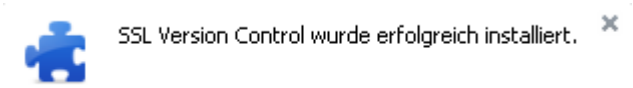
Das Add-on wird **heruntergeladen**

SSL 3.0 deaktivieren – Sicherheitslücke „Poodle“

Die Installation des Add-on starten wir durch einen Klick auf > **jetzt installieren**

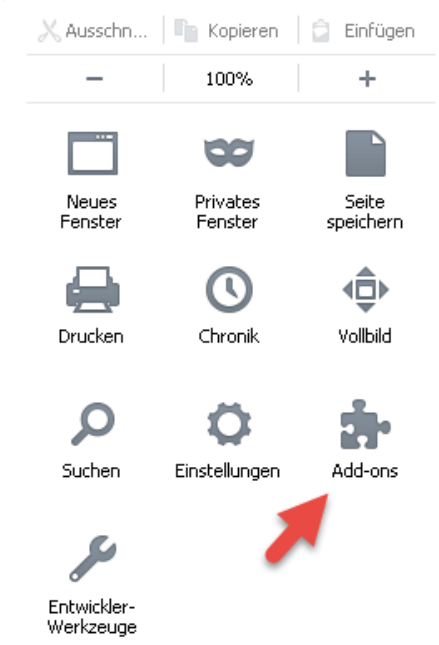


Nach der Installation bekommen wir einen Status angezeigt.

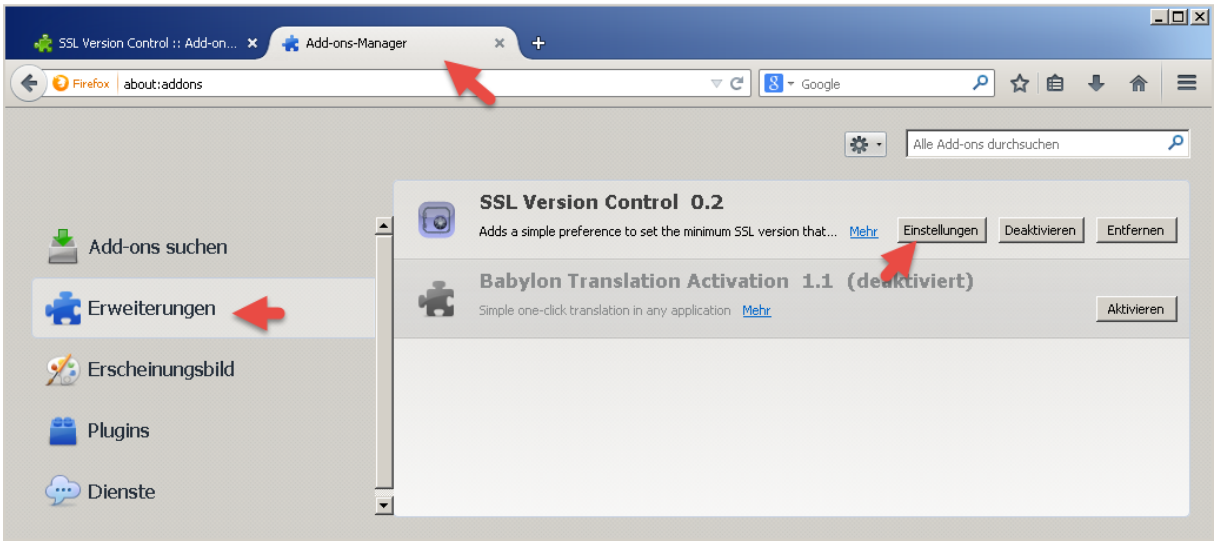


Ab jetzt **akzeptiert Firefox** nur das sichere **TLS** ab Versionen 1.0 und aufwärts.

Das Add-on öffnen Sie über **Einstellungen > Add-ons**



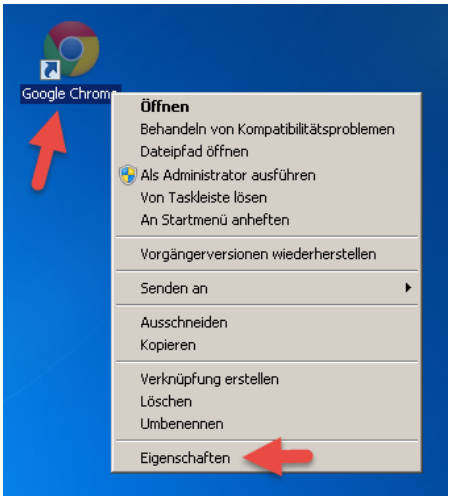
SSL 3.0 deaktivieren – Sicherheitslücke „Poodle“



Mit einem Klick auf **Einstellungen** öffnet sich die Schaltzentrale

- **Chrome**

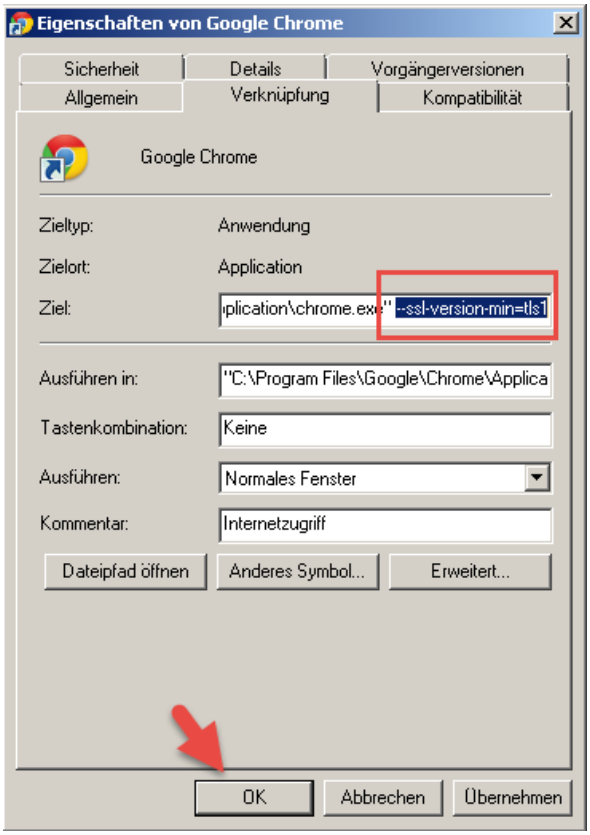
Mit einem **Rechtsklick** auf die **Verknüpfung** zu Google Chrome öffnen wir die **Eigenschaften**



In der Zeile Ziel **erweitern** wir den Befehl um folgenden String:
--ssl-version-min=tls1

"C:\Program Files\Google\Chrome\Application\chrome.exe" **--ssl-version-min=tls1**

Achten Sie auf das Leerzeichen.



Und schließen die Änderung mit einem Klick auf **> OK** ab.

Jetzt arbeiten alle 3 Browser mit dem sicheren TLS (Transport Layer Security).