# Anpassung der Internet Explorer Einstellungen

## *Internet & E-Mail á Microsoft*

Der Internet Explorer macht immer wieder durch schwere Sicherheitslücken auf sich aufmerksam. Doch selbst wer sicherere Alternativen wie Opera verwendet, kann über die Hintertür immer noch Gefahren ausgesetzt sein, wenn als E-Mail Programm eines der Microsoft Programme Outlook, Outlook Express oder Windows Mail zum Einsatz kommt. Diese E-Mailer verwenden den Internet Explorer zum anzeigen von HTML Mails, und bieten deshalb oft dieselben Schwachstellen wie der Browser. Zudem gelten die Sicherheitseinstellungen für Browser und E-Mail Programm gleichermaßen, weshalb wir auch die Browser-Einstellungen ändern müssen, um die E-Mail Programme abzusichern.

## *Aktiver Ärger*

Eines der Hauptprobleme sind die sogenannten ActiveX Plugins für den Internet Explorer. Beinahe jede Woche kommt ein anderes Plugin ins Visier der Sicherheitsexperten, und meistens hat der jeweilige Hersteller keine Sicherheitsupdates parat, weshalb die unzufriedenstellende Problemlösung lautet, ein sogenanntes „KillBit“ zu setzen, was die Ausführung des fehlerhaften Plugins verhindert. Leider ist diese Vorgehensweise für normale Anwender viel zu kompliziert, und selbst wer kein Problem hätte diesen Eingriff einmal zu machen, wird nach dem x-ten unsicheren Plugin entnervt aufgeben.

## *Die Lösung?*

Wenn es also zu viel Aufwand bedeutet, jedes fehlerhafte Plugin einzeln zu deaktivieren, dann hilft nur mehr die vollständige Deaktivierung aller Plugins für den Internet Explorer. Genau das beschreiben wir im Folgenden. Doch eines sei zuvor gesagt, ein Internet Explorer, der keine Plugins mehr ausführen darf, ist für alltägliches surfen im Internet kaum mehr zu gebrauchen. Spätestens dann führt also kein Weg mehr an einem alternativen Browser vorbei. Zum Glück ist das keine Einschränkung, denn Opera (unsere klare Empfehlung) ist dem Internet Explorer in jeder Hinsicht weit überlegen. Nur schlecht programmierte Webseiten, die eben solche unsicheren ActveX Plugins erfordern, können mit alternativen Browsern nicht, oder nur mit Einschränkungen benutzt werden.

## *Keine Regel ohne Ausnahme*

Die wohl bekannteste „schlecht programmierte“ Webseite, ist „Windows Update“ bzw. „Microsoft Update“. Microsoft ist wohl nicht auf die Idee gekommen, dass ein Windows Anwender einen alternativen Browser dazu verwenden möchte, um sich Updates für Windows herunterzuladen. Und so zündet Microsoft bei den Webseiten ein wahres Feuerwerk an ActiveX Plugins. Nur wenn alle davon akzeptiert und installiert werden, funktioniert das Update über die Webseiten. Um manuell nach Updates für die Microsoft Programme suchen zu können, muss man daher der Update Webseite den Zugriff auf die Plugins gestatten. Das funktioniert im Internet Explorer dank des Zonenmodells, dass Webseiten zu unterschiedlichen Gruppen zusammenfassen kann. Standardmäßig wird jede Webseite der Zone „Internet“ zugeordnet. Für diese Zone verbieten wir aber die Verwendung von ActiveX, weshalb Microsofts Update Webseiten in eine andere Zone eingetragen werden müssen, in der nicht so strenge Regeln gelten. Wir verwenden dafür im Folgenden die Zone „vertrauenswürdige Webseiten“. Zwar hat nicht jedermann wirklich vertrauen zu Microsoft, aber die Frage lautet eben: „Updates oder nicht?“. Wer welche haben möchte, sollte die genannten Adressen der Liste hinzufügen:

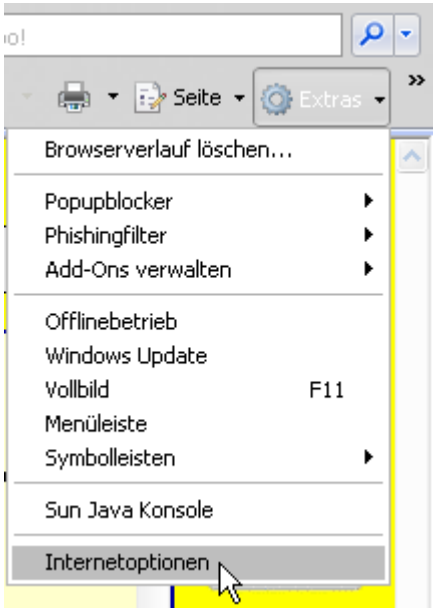
- http://update.microsoft.com
- http://*.update.microsoft.com
- https://*.update.microsoft.com
- http://download.windowsupdate.com

Dasselbe gilt für eventuelle Intranet Seiten des Arbeitgebers. Funktionieren diese nur in Verbindung mit dem Internet Explorer, muss man auch diese zur passenden Zone, in dem Fall „Lokales Intranet“, hinzufügen. Aber Vorsicht, fügen Sie nur Webseiten zu einer der beiden Zonen hinzu, die sie als absolut vertrauenswürdig erachten. Leichtfertiges hinzufügen von allerlei Webseiten kann letztendlich das Sicherheitsrisiko steigern statt senken, womit sich die Aktion ad absurdum führen würde.

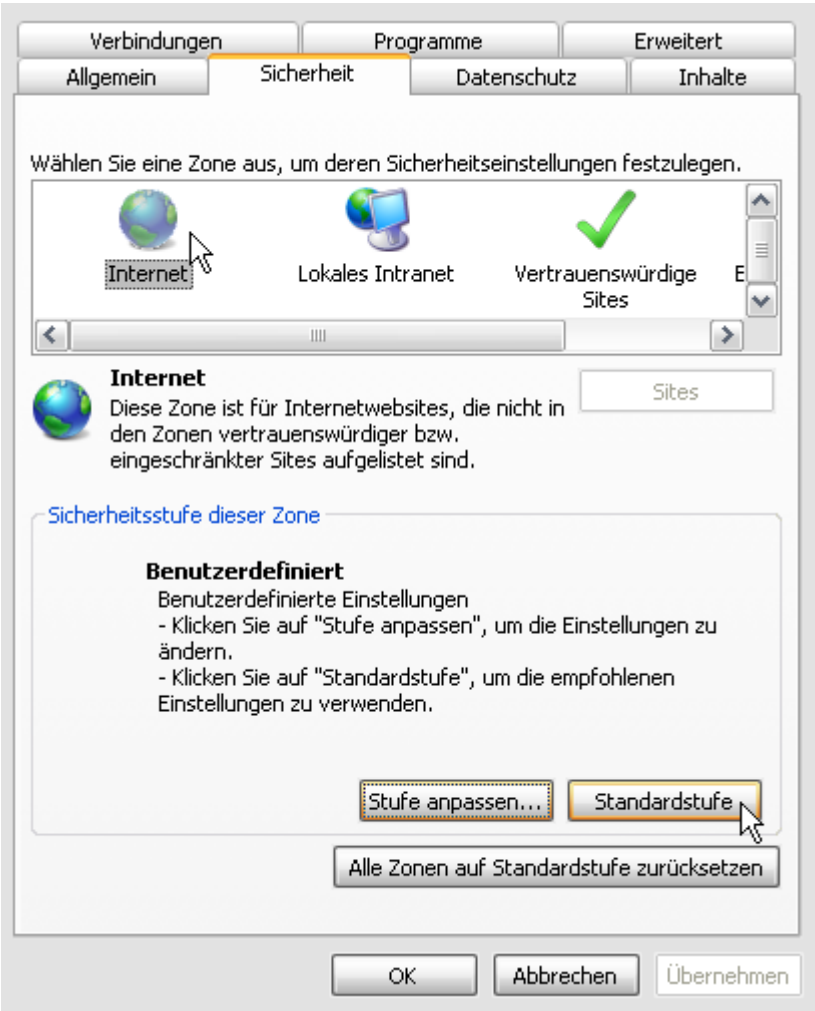
## *Detaillierte Anleitung:*

Ein Bild sagt mehr als tausend Worte, weshalb wir jetzt die Prozedur Schritt für Schritt durchgehen. Doch bevor wir loslegen noch ein Tipp für alle Anwender von Windows Vista: Laden sie alle Windows Updates herunter, **bevor** sie diese Anleitung durchführen.

Wir gehen davon aus, dass der Internet Explorer bereits gestartet ist, und öffnen nun das Einstellungen Fenster, indem wir rechts auf „Extras“ klicken. Beim Internet Explorer 6 findet sich der Eintrag oben in der Menüleiste.

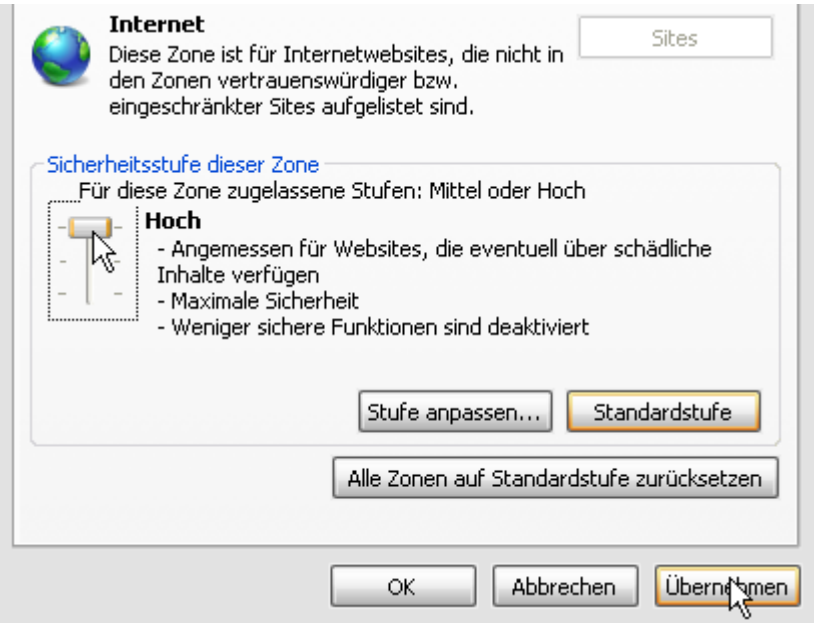



Im sich öffnenden Fenster klicken wir zuerst auf den Karteireiter Sicherheit, und wählen dann die Internetzone aus, indem wir auf das Weltkugel Symbol klicken.




Falls, so wie hier, die Regler für die Sicherheit nicht angezeigt werden, klicken wir zuerst auf „Standardstufe“ um diese wieder anzuzeigen.

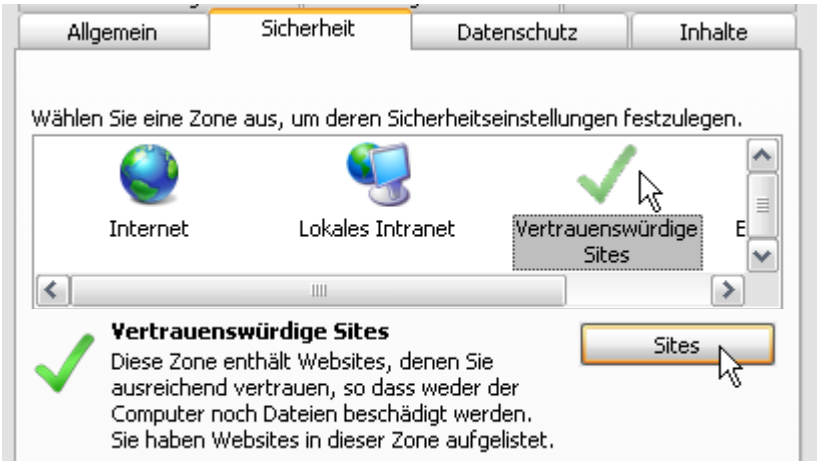
Man könnte jetzt auf „Stufe anpassen“ klicken, und unzählige Einträge von ActiveX von Hand auf „deaktiviert“ setzen, doch wir sparen uns den Aufwand, und setzen die Sicherheitsstufe einfach auf „Hoch“, womit ebenfalls ActiveX für diese Zone ausgeschaltet wird.




Anschließend klicken wir auf „Übernehmen“, um den ersten Schritt der Aufgabe zu speichern.

Als nächstes sorgen wir dafür, dass die Update Webseiten von Microsoft weiterhin funktionieren.

Anwender von Windows Vista können sich die folgenden Schritte sparen, wenn sie den Tipp ganz am Anfang befolgt, und alle Windows Updates heruntergeladen haben. Die aktuellste Fassung von „Windows Update“ von Windows Vista ignoriert nämlich die Einstellung des Internet Explorer.



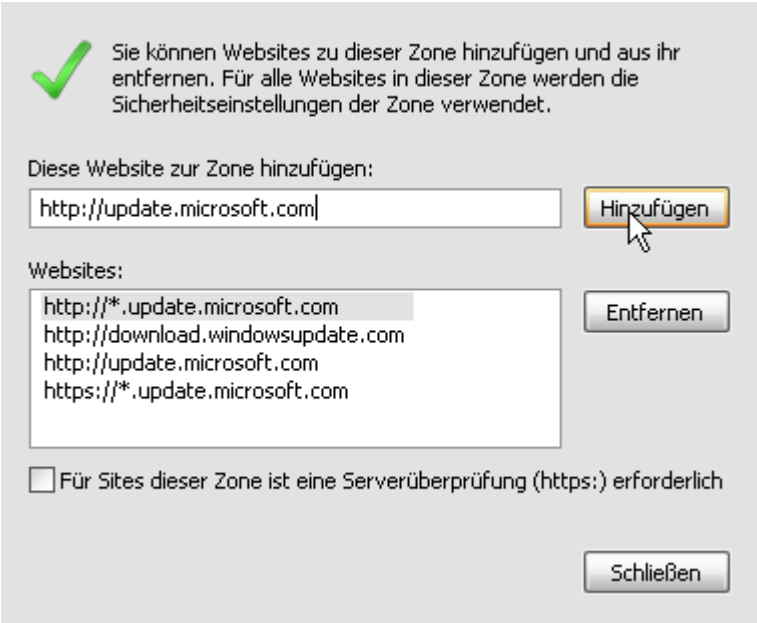

Anwender von Windows XP (für Windows 2000 sollte das auch noch gelten) fahren fort, indem sie die Zone „Vertrauenswürdige Sites“ auswählen (anklicken).

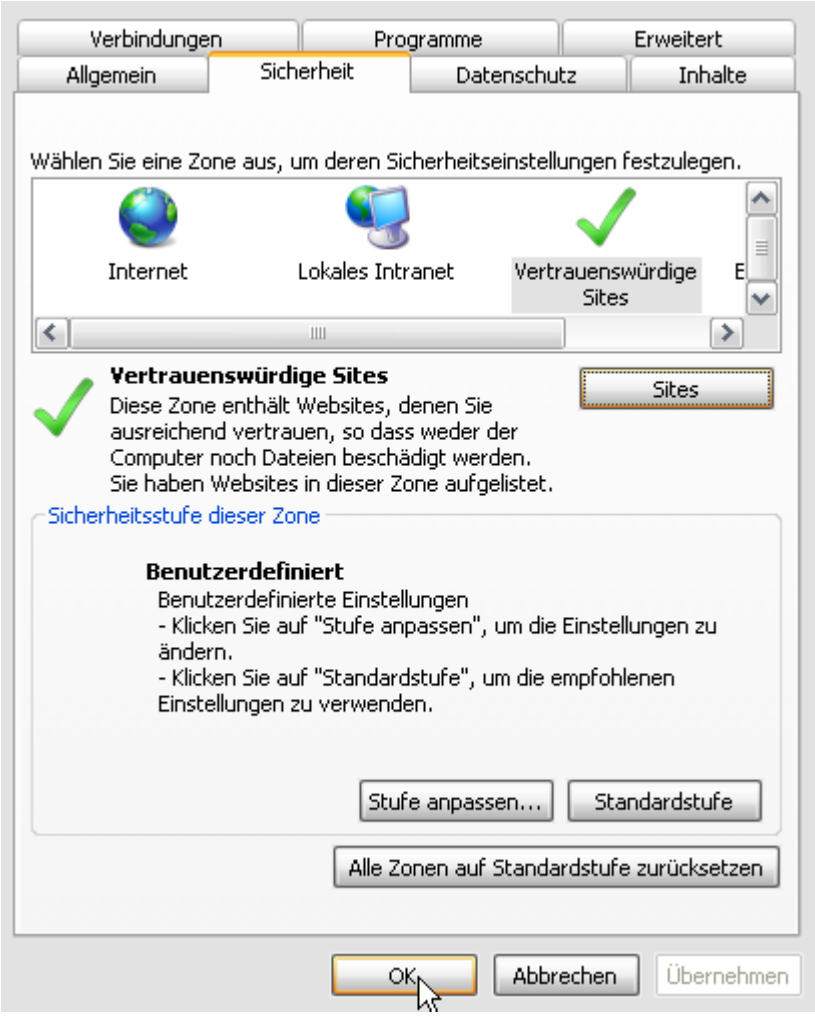
Danach klicken wir auf die Schaltfläche „Sites“.

Um in dem sich öffnenden Fenster alle nötigen Adressen eingeben zu können, muss zuerst das Häkchen vor „*Für Sites dieser Zone ist eine Serverüberprüfung (https:) erforderlich*“ entfernt werden.

Jetzt trägt man der Reihe nach die Adresse ein, und klickt auf „hinzufügen“.

Sind alle Adressen wie auf dem Bild eingefügt, schließt man da Fenster mit einem Klick auf „Schließen“.






Ein letzter Klick auf „OK“, und das wars auch schon.

Die Sicherheitsstufe „Hoch“ in der Zone „Internet“ sorgt dafür, dass ActiveX Plugins in Webseiten und E-Mails nicht mehr gestartet werden können, womit sie auch keinen Schaden anrichten können.

Die Aufnahme der Microsoft Seiten zur Zone der „Vertrauenswürdigen Sites“ sorgt dafür, dass „Windows-“ bzw. „Microsoft Update“ weiterhin Funktionsfähig bleibt.

Claus Berghammer
CB Computerservice
Web: www.cb-computerservice.at
Mail: office(at)cb-computerservice.at
Mobil: 0660 / 8143685
Hallwanger Landesstraße 2
5300 Hallwang bei Salzburg