Die wichtigsten Einstellungen des Internet Explorer 7 auf einen Blick

.NET Framework - XAML

XAML ist eine Microsoft-Technologie, über die verschiedene Animationen in Webseiten eingebunden werden können. Hier besteht das Risiko, dass diese Websprache, die Flash ähnlich ist, in naher Zukunft von Hackern missbraucht wird, um Viren oder Spyware auf den Computer zu übertragen. Wir empfehlen daher, die entsprechenden Optionen zu deaktivieren, wenn Sie auf Nummer sicher gehen wollen, auch wenn im Moment noch keine Gefahr besteht, da es kaum XAML-Websites gibt.

ActiveX - für Scripting sicher

Wer auf Sicherheit achtet, sollte vor allem die Einstellungen für ActiveX und Active Scripting modifizieren, da insbesondere diese Techniken bei Angriffen missbraucht werden: Wer ganz sichergehen will, deaktiviert auch die sicher klassifizierten Steuerelemente; die Option "Bestätigen" ist aber die sinnvollere Option.

Steuerelemente & Plug-ins ausführen

Deaktivieren Sie diese Option, werden auch hilfreiche Steuerelemente nicht mehr ausgeführt - beispielsweise werden PDFs nicht mehr im Browser dargestellt. Die "Bestätigen"-Option ist hier die bessere Wahl.

Scripting - Active Scripting

Microsofts Alternative zu JavaScript ist zu anfällig für Attacken - schalten Sie die Option ab. "Bestätigen" hätte zur Folge, dass Sie permanent Warnfenster wegklicken müssten.

Verschiedenes - Domänengrenzen

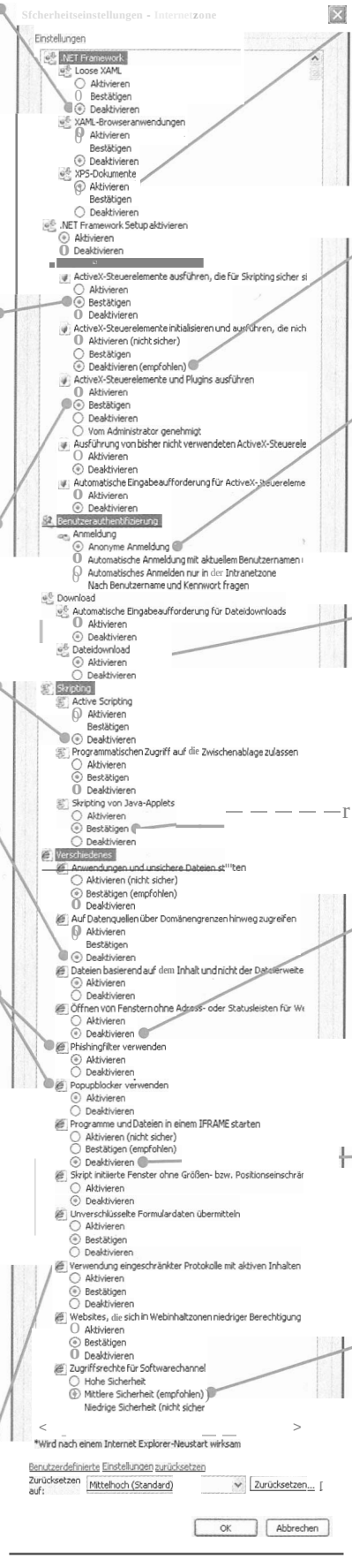
Nur wenn Sie sich neben dem Internet auch in einem Intranet bewegen, müssen Sie auf Daten von fremden Domänen zugreifen und würden "Bestätigen" wählen. Andernfalls deaktivieren Sie diese Option.

Phishing-Filter & Pop-up-Blocker

Aktivieren Sie den Phishing-Filter. Er vergleicht nun die Adressen der besuchten Websites mit einer Liste von Seiten, die Microsoft als legitime Sites gemeldet wurden und die auf Ihrem Computer gespeichert sind. Nicht bekannte Seiten übermittelt er an Microsoft zur Überprüfung und analysiert die Sites außerdem daraufhin, ob sie die üblichen Merkmale einer Phishing-Seite aufweisen. Etwas zu rigoros geht der IE7 mit Pop-up-Fenstern um: Wählen Sie "Extras/Popupblocker/Popupblocker-Einstellungen" und entscheiden Sie sich für "Niedrig: Popups von sicheren Sites zulassen." So können sichere Websites, die das https:l/-Protokoll verwenden - beispielsweise Banken und Sparkassen - automatisch Pop-up-Fenster öffnen, ohne dass Sie diese Sites zur Liste "Zugelassene Sites" hinzufügen müssen.

Unverschlüsselte Formulardaten

Damit beispielsweise bei Formularen von Onlineshops nur Daten versendet werden, wenn Sie dies auch wirklich bewusst wünschen, wählen Sie die Option "Bestätigen".



.NET Framework - XPS

Durch die Option zu XPS-Dokumenten lässt sich der im IE7 integrierte XPS-Viewer deaktivieren, sodass Sie die Dokumente, die eine Alternative zum PDF-Format sind, nicht mehr im Internet Explorer betrachten können. Da dies lediglich eine Beschränkung des Surfkomforts bedeuten würde, können Sie diese Option bis auf Weiteres aktivieren.

ActiveX – nicht sicher für Scripting

Deaktivieren Sie die Option "ActiveX-Steuerelemente ausführen, die nicht als sicher für Skripting markiert sind" - denn unsichere ActiveX-Steuerelemente haben auf Ihrem System nichts zu suchen.

Benutzerauthentifizierung

Teilweise müssen Sie sich auf Internetseiten als User verifizieren. Dabei kann der IE Ihre Userdaten automatisch mit den Standardauthentifizierungsinformationen einer verschlüsselten Seite übermitteln. Wählen Sie "Anonyme Anmeldung", damit Ihre Daten keinesfalls unbemerkt an andere übertragen werden.

Download - Dateien

Mit dieser Option stellen Sie ein, ob Downloads von Dateien aus dem Internet möglich sein sollen. Falls Sie diese Option deaktivieren, ist der Download allerdings völlig unmöglich. Für eine sinnvolle Internetnutzung müssen Sie die Option aktivieren.

Scripting - Java-Applets

Damit Java-Applets nicht unkontrolliert auf Ihrem Rechner operieren können, empfehlen wir Ihnen, diese zunächst "Bestätigen" zu müssen.

Verschiedenes - Fenster ohne Leiste

Die Optionen "Öffnen von Fenstern ohne Adress- und Statusleisten zulassen" sowie "Skript initiierte Fenster ohne Größen- und Positionseinschränkung zulassen" sollten deaktiviert sein. Denn Hacker versuchen durch verschiedene Tricks, aktive Inhalte zum Laufen zu bringen, beispielsweise durch nicht sichtbare, nur ein Pixel große Fenster.

Programme in einem IFRAME

Im Unterschied zu herkömmlichen Frames können in IFRAMES auch fremde Dateien oder Links aufgerufen werden - eine potenziell gefährliche Angelegenheit, schließlich wissen Sie nie, um welche Seite oder Datei es sich handelt. Deaktivieren Sie deshalb diese Option besser.

Zugriffsrechte für Softwarechannel

Über den Softwarechannel werden Programme auf Ihren Rechner übertragen. Da Programme mit Viren infiziert sein oder Trojaner beheimaten können, sollten Sie genau darauf achten, welche Programme auf Ihren Rechner gelangen und woher. Die Einstellung "mittlere Sicherheit" ist zu empfehlen, da hierbei beispielsweise Updates nur nach vorheriger Rückfrage erfolgen.