Besser geschützt mit dem kostenlosen EMET Sicherheitstool von Microsoft

Teil 1
Versionen: Excel 2013, 2010, 2007, 2003 und 2002/XP

Jeden Monat bringt Microsoft neue Updates heraus, die Ihr System sicherer und stabiler machen. Die Updates stopfen allerdings nur Sicherheitslücken, die bereits bekannt sind. Doch auch gegen potenzielle neue Gefahren hat Microsoft ein Mittel: EMET, das "Enhanced Mitigation Experience Toolkit". Es blockt Angriffe schon beim Versuch, schadhaften Code auszuführen. Gerade erst ist die neueste Version von EMET erschienen. Grund genug, das Toolkit näher vorzustellen.

Windows besitzt spätestens seit Windows Vista verschiedene Sicherheitsmechanismen, die das Einschleusen von Viren und Malware erschweren. Aber längst nicht jedes Programm setzt diese Mechanismen effektiv ein, insbesondere Programme, die älteren Datums sind. So entstehen Sicherheitslücken, die Hacker nur zu gerne ausnutzen. Selbst aktuelle Programme sind nicht vor solchen Sicherheitslücken gefeit, wie unter anderem die monatlichen Sicherheitsupdates von Microsoft belegen.

Was also tun gegen die Gefahren, die im Internet und in fremden E-Mails oder Arbeitsmappen bzw. Dokumenten lauern? Neben der Installation der jüngsten Programm-Updates ist natürlich ein Antivirenprogramm unerlässlich, das Sie immer auf dem neuesten Stand halten. Aber es geht noch besser: Schützen Sie Ihr System mit dem "Enhanced Mitigation Experience Toolkit", kurz: EMET.

EMET kann Ihr System auch vor Angriffen schützen, die bislang unbekannte Sicherheitslücken ausnutzen. Dazu muss man wissen, dass Viren und Trojaner oft nach demselben Prinzip vorgehen. Sie suchen Schwachstellen in regulärem Programmcode, um den eigenen, schadhaften Code im Arbeitsspeicher zu platzieren und ihn dann auszuführen. EMET überwacht derartige Muster und verhindert die Ausführung von Codebestandteilen, die verdächtig erscheinen.

Im Gegensatz zu Antivirenprogrammen versteht sich EMET aber nicht als Pauschalschutz Ihres Systems. EMET arbeitet programm- bzw. prozessorientiert, das heißt, es klinkt sich konkret in die Abläufe eines Programms ein und unterbricht die Programmausführung, falls Code aufgerufen wird, der so nicht vorgesehen ist. Dabei spielt es keine Rolle, ob es sich um ein Microsoft-Programm handelt oder um Software von anderen Herstellern.

Das Ganze passiert unmerklich im Hintergrund. Sie müssen EMET nur mitteilen, welche Programme überwacht werden sollen und wie weit die Schutzmaßnahmen reichen sollen.

Wenn Sie jetzt immer noch Zweifel haben, ob Sie EMET wirklich brauchen, dann überzeugt Sie vielleicht das Kostenargument: EMET kostet Sie nichts! Das Setup-Programm der aktuellen EMET-Version 4.1 können Sie frei von folgender Microsoft-Seite herunterladen:

[**http://www.microsoft.com/en-us/download/details.aspx?id=41138**](http://www.microsoft.com/en-us/download/details.aspx?id=41138)

Nach einem Klick auf den *Download*-Button wählen Sie am besten sowohl die Setup-Datei als auch die PDF-Datei des Benutzerhandbuchs zum Download aus und danach speichern Sie die Dateien auf Ihrer Festplatte.

Bevor Sie EMET 4.1 sofort installieren, beachten Sie bitte folgende Dinge:

* Wenn auf Ihrem System bereits eine ältere EMET-Version läuft, müssen Sie diese erst deinstallieren. Damit Sie Ihre bisherigen Schutzeinstellungen nicht verlieren, exportieren Sie sie vorher in eine Konfigurationsdatei (XML-Datei).
* EMET kann dazu führen, dass einzelne Programme nicht mehr reibungslos funktionieren. Das lässt sich meist durch Lockerungen der jeweiligen Schutzeinstellungen beheben. Trotzdem sollten Sie EMET erst in einer Testumgebung ausprobieren, bevor Sie Ihren "echten" Büro- bzw. Heim-PC damit schützen.
* EMET 4.1 setzt das .NET-Framework 4 voraus, welches auf neueren Windows-Versionen üblicherweise vorhanden ist. Ansonsten werden Sie während der EMET-Installation dazu aufgefordert, das .NET-Framework aus dem Internet zu laden.

Damit wären wir bei der Installation von EMET 4.1. Die gestaltet sich so einfach, dass sie auch von unerfahrenen Anwendern problemlos bewältigt werden kann: Starten Sie die heruntergeladene Datei "EMET Setup.msi" und gehen Sie den Installationsassistenten Schritt für Schritt durch.

Am Ende werden Sie nach der Konfiguration gefragt. Aktivieren Sie die Option *Use Recommended Settings* und klicken Sie danach auf *Finish*.

Nach der Installation schützt EMET Ihre Microsoft Office-Anwendungen sowie den Internet Explorer, Adobe Acrobat/Reader und Java-Anwendungen.

Um das Feintuning kümmern wir uns im zweiten Teil dieses Tipps.

Besser geschützt mit dem kostenlosen EMET-Sicherheitstool von Microsoft, Teil 2
Versionen: Excel 2013, 2010, 2007, 2003 und 2002/XP

Ihr PC ist permanent durch Viren, Trojaner oder andere Schadsoftware bedroht. Mit EMET, dem kostenlosen "Enhanced Mitigation Experience Toolkit" von Microsoft, erweitern Sie den Schutz vor solchen Angriffen um eine besonders effektive Komponente. Im ersten Teil dieses Tipps hatten wir erklärt, wie EMET funktioniert und wie Sie das Toolkit auf Ihrem PC installieren. Erfahren Sie nun mehr über die Konfiguration der Schutzfunktionen.

EMET wird automatisch zusammen mit Windows gestartet. Sie müssen nichts weiter machen, damit EMET seine Schutzfunktion erfüllt. Bemerkbar macht sich das Toolkit nur, wenn tatsächlich verdächtige Aktionen ausgeführt werden. Dann meldet sich in der Regel der "EMET Notifier" über dem Infobereich der Windows-Taskleiste und das Programm, in dem eine Bedrohung festgestellt wurde, wird automatisch beendet.

EMET besitzt aber auch eine grafische Benutzeroberfläche zur individuellen Anpassung der Konfiguration. Der Aufruf erfolgt entweder über den Infobereich der Taskleiste, in dem Sie doppelt auf das Symbol des *EMET Notifier* klicken, oder über das Windows-Startmenü bzw. den Startbildschirm von Windows 8, von wo Sie das Programm *EMET Gui* starten.

Der Programmbildschirm von EMET enthält ein Menüband, einen Statusbereich und eine Liste der laufenden Windows-Prozesse. Interessant an der Liste ist, dass Sie an einem Symbol in der Spalte *Running EMET* sofort erkennen, ob ein Programm von EMET überwacht wird.

Zur Ansicht aller geschützten Programme klicken Sie im Menüband in der Gruppe *Configuration* auf *Apps*. Daraufhin öffnet sich ein neues Fenster mit einer Liste der unterstützten Programme.

Wenn Sie bei der EMET-Installation die empfohlene Konfiguration aktiviert hatten, gehören unter anderem alle Microsoft Office-Anwendungen dazu. Die Häkchen rechts daneben zeigen an, welche Schutzfunktionen aktiviert sind. Was DEP (Data Execution Prevention), BottomUpASLR (Bottom Up Address Space Layout Randomization) usw. konkret bewirken, ist in erster Linie für Insider oder technisch versierte Anwender interessant. Wichtig ist nur, dass Sie bei jedem Programm bestimmen können, wie umfangreich der Schutz sein soll.

Solange die Programme mit den Standardeinstellungen reibungslos funktionieren, ändern Sie daran nichts. Es kann aber sein, dass der EMET-Schutz die Ausführung bestimmter Programme beeinträchtigt.

So stellen Sie bei der Arbeit in Ihrer Office-Anwendung oder in einem anderen von EMET überwachten Programm womöglich fest, dass das Programm bei ganz normalen Benutzeraktionen abstürzt. Wenn Sie ausschließen können, dass dieses Verhalten auf den Aufruf einer infizierten Webseite oder das Öffnen eines virenverseuchten Dokuments zurückzuführen ist, überprüfen Sie, ob es an EMET liegt:

1. Starten Sie die EMET-Benutzeroberfläche und öffnen Sie mit einem Klick auf *Apps* das Fenster *Application Configuration*.
2. Klicken Sie mit der rechten Maustaste auf den Namen der betroffenen Programmdatei und deaktivieren Sie über den Kontextmenübefehl *Disable All Mitigations* alle Schutzfunktionen.
3. Starten Sie die Anwendung, deren Schutzfunktionen Sie deaktiviert haben, und prüfen Sie, ob es weiterhin zu Problemen kommt.
4. Wenn das der Fall ist, ist EMET nicht schuld, da der Schutz des Toolkits ausgeschaltet ist. Sie können ihn dann wieder einschalten, indem Sie die vorherigen Schritte wiederholen und dieses Mal den Kontextmenübefehl *Enable All Mitigations* anwählen.

Sollten die Probleme durch das Deaktivieren von EMET aber verschwinden, müssen Sie einzeln prüfen, welche Schutzfunktion das Fehlverhalten verursacht hat. Schalten Sie im Fenster *Application Configuration* nach und nach eine zusätzliche Schutzfunktion in der Zeile des betreffenden Programms ein und prüfen Sie jedes Mal, ob der zuvor beobachtete Fehler auftritt. Lassen Sie am Ende nur die Schutzfunktion(en) ausgeschaltet, die die normale Programmfunktionalität beeinträchtigen.

Praktisch ist, dass Sie den EMET-Schutz auf jedes beliebige Programm ausdehnen können. Wenn Sie zum Beispiel viel mit Google Chrome im Internet surfen, fügen Sie die entsprechende Programmdatei einfach zur Liste der Apps hinzu:

1. Öffnen Sie über die EMET-Benutzeroberfläche wieder das Fenster *Application Configuration*.
2. Klicken Sie im Menüband in der Gruppe *Add/Remove* auf *Add Application*.
3. Suchen Sie die Programmdatei "chrome.exe" auf Ihrem Computer und wählen Sie sie per Doppelklick aus. Wenn Sie den Installationsordner kennen, können Sie natürlich auch manuell in diesen Ordner wechseln und die Programmdatei per Doppelklick öffnen.
4. EMET trägt das neue Programm sofort in seine Apps-Liste ein und aktiviert alle Schutzfunktionen. Akzeptieren Sie dies mit einem Klick auf *Ok*.
5. Testen Sie, ob das Programm - in diesem Fall Google Chrome - mit den EMET-Schutzeinstellungen funktioniert. Bei Inkompatibilitäten müssen Sie, wie oben beschrieben, einzelne Schutzfunktionen deaktivieren. Speziell bei Chrome muss der "SEHOP"-Schutz ausgeschaltet werden.

Sie sehen, EMET ist recht einfach zu konfigurieren und bietet weit reichenden Schutz vor diversen Angriffen auf Ihren PC. Noch dazu ist es kostenlos. Somit gibt es eigentlich keinen Grund, auf EMET zu verzichten.